

# The Fundamental Theorems of Vector Invariants

DAVID R. RICHMAN

*Department of Mathematics, University of South Carolina,  
Columbia, South Carolina 29208*

New proofs are given of the First Fundamental Theorems of vector invariants for the special linear and special orthogonal groups. The novelty of the proofs is that they rely on reducing the theorems to the case of  $2 \times 2$  matrices; there is a close connection between the vector invariants of the special linear group or special orthogonal group of  $n \times n$  matrices, for all  $n \geq 2$ , and those of the analogous group of  $2 \times 2$  matrices. This connection is described using the notion of leading monomials. Properties of leading monomials are also used to give new proofs of the Second Fundamental Theorems of vector invariants for the general linear and orthogonal groups. © 1989 Academic Press, Inc.

## 1. INTRODUCTION

*Notation.* Let  $F$  denote an infinite field and let  $C_{ij}$  and  $X_{uv}$ , where  $1 \leq i \leq m$ ,  $1 \leq j \leq n$ , and  $1 \leq u \leq p$ , denote commuting indeterminates. Let  $F[C, m \times n; X, p \times n]$  denote the polynomial ring generated by the  $C_{ij}$ 's and  $X_{uv}$ 's and let  $F[C, m \times n]$  denote the polynomial ring generated by the  $C_{ij}$ 's.

If  $g$  denotes an invertible  $n \times n$  matrix with entries in  $F$ , let  $C_{ij}^g$  and  $X_{ij}^{g*}$  denote the elements of  $F[C, m \times n; X, p \times n]$  which satisfy the matrix equations

$$(C_{i1}^g C_{i2}^g \cdots C_{in}^g) = (C_{i1} C_{i2} \cdots C_{in}) g$$

and

$$(X_{i1}^{g*} X_{i2}^{g*} \cdots X_{in}^{g*}) = (X_{i1} X_{i2} \cdots X_{in}) (g^{-1})^T$$

for all  $i$ . If  $f = f(C_{11}, \dots, C_{mn}, X_{11}, \dots, X_{pn})$  denotes an element of  $F[C, m \times n; X, p \times n]$ , define

$$f^g = f(C_{11}^g, \dots, C_{mn}^g, X_{11}^{g*}, \dots, X_{pn}^{g*}).$$

**DEFINITION.** Let  $G$  denote a set of invertible  $n \times n$  matrices with entries in  $F$ . An element  $f$  in  $F[C, m \times n; X, p \times n]$  is said to be an absolute vector covariant of  $G$  if  $f = f^g$  for all  $g$  in  $G$ . An absolute vector covariant of  $G$  which lies in  $F[C, m \times n]$  is said to be an absolute vector invariant of  $G$ .

In this paper, an absolute vector covariant of  $G$  will be referred to simply as a covariant of  $G$ , and an absolute vector invariant of  $G$  will be referred to simply as an invariant of  $G$ .

*Notation.* Let  $GL(n, F)$  denote the group of invertible  $n \times n$  matrices whose entries lie in  $F$ . Let  $SL(n, F)$  denote the group of matrices in  $GL(n, F)$  of determinant 1 and let  $O(n, F)$  denote the group of matrices  $B$  in  $GL(n, F)$  which satisfy  $BB^T = I$ . Let  $SO(n, F) = O(n, F) \cap SL(n, F)$ .

Let  $C_{m \times n}$  denote the  $m \times n$  matrix whose  $(i, j)$ th entry is  $C_{ij}$  for all  $i, j$  and let  $X_{p \times n}$  denote the  $p \times n$  matrix whose  $(i, j)$ th entry is  $X_{ij}$  for all  $i, j$ .

The First Fundamental Theorem of vector invariants for  $SL(n, F)$  states that the set of invariants of  $SL(n, F)$  in  $F[C, m \times n]$  is generated as an  $F$ -algebra by the  $n \times n$  minors of  $C_{m \times n}$ . In the case that the characteristic of  $F$  equals zero, this theorem is proved by Turnbull in [20]; the case  $n = 2$  had been proved earlier by Clebsch (cf. [3, 11, 12]). Proofs which are valid for fields of characteristic zero are also given in [7, 10, 21]. The first proof which is valid for all infinite fields is given by Igusa in [15]; his proof uses concepts of algebraic geometry. An elementary proof is sketched by Doubilet, Rota, and Stein in [8], and a complete, elementary proof is given by Désarménien, Kung, and Rota in [6]. Other proofs which are valid for all infinite fields are given by Barnabei and Brini in [2] and by deConcini and Procesi in [5].

The First Fundamental Theorem of vector covariants for  $SL(n, F)$  states that the set of covariants of  $SL(n, F)$  in  $F[C, m \times n; X, p \times n]$  is generated as an  $F$ -algebra by the  $n \times n$  minors of  $C_{m \times n}$ , the  $n \times n$  minors of  $X_{p \times n}$ , and the entries of the matrix product  $C_{m \times n} X_{p \times n}^T$ . In the case that the characteristic of  $F$  equals zero, this theorem is proved in the books of Turnbull [20] and Weyl [21]. In [5], deConcini and Procesi establish the theorem for all infinite fields  $F$ .

Suppose that the characteristic of  $F$  is different from two. The First Fundamental Theorem of vector invariants for  $SO(n, F)$  states that the set of invariants of  $SO(n, F)$  in  $F[C, m \times n]$  is generated as an  $F$ -algebra by the  $n \times n$  minors of  $C_{m \times n}$  and the polynomials of the form  $C_{i1}C_{k1} + C_{i2}C_{k2} + \cdots + C_{in}C_{kn}$ . This theorem is proved by Weyl in [21] for fields of characteristic 0 and by deConcini and Procesi in [5] for infinite fields of characteristic different from two. Analogous results for the symmetric and symplectic groups are also bound in [5, 21]. In [21] there are also general results about vector invariants of groups of lower triangular matrices.

This paper presents new proofs of the First Fundamental Theorems of vector covariants for  $SL(n, F)$  and of vector invariants for  $SO(n, F)$ . The novelty of the proofs is that they rely on reducing the theorems to the case  $n = 2$ . In Section 2 it is shown that there is a close connection between the

leading monomials of covariants of  $SL(n, F)$ , for all  $n \geq 2$ , and those of  $SL(2, F)$ . In Section 3 these results are used to establish the First Fundamental Theorem of vector covariants for  $SL(n, F)$ , and to show that the covariants of the group of upper triangular matrices in  $SL(n, F)$  are the same as those of  $SL(n, F)$ . Section 4 contains a proof of the First Fundamental Theorem of vector invariants for  $SO(n, F)$ , where  $F$  denotes an infinite field of characteristic different from two. Section 5 contains a proof that, when  $F$  is an infinite field of characteristic two, the set of invariants of  $O(n, F)$  in  $F[C, m \times n]$  is generated as an  $F$ -algebra by the elements  $C_{i1} + C_{i2} + \dots + C_{in}$  and  $C_{i1}C_{k1} + C_{i2}C_{k2} + \dots + C_{in}C_{kn}$ , where  $i$  and  $k$  range over the set  $\{1, \dots, m\}$ . This result is new; an incorrect theorem about the invariants of  $O(n, F)$  is given in [5, pp. 353–354].

Given a finite set  $\{f_1, \dots, f_N\}$  of generators of the vector covariants of a set  $G \subseteq GL(n, F)$ , a Second Fundamental Theorem of vector covariants for  $G$  is a theorem which describes generators for the ideal of polynomials  $p(X_1, \dots, X_N)$  which satisfy  $p(f_1, \dots, f_N) = 0$ . The Second Fundamental Theorems of vector covariants for  $GL(n, F)$  and  $SL(n, F)$  were first proved by E. Pascal in [18]; other proofs for  $GL(n, F)$  are found in [1, 4, 5, 6, 13, 17, 21]. Second Fundamental Theorems for covariants of  $SL(n, F)$ ,  $O(n, F)$ , and the symplectic group are given in [5, 21]. Most proofs of these results use Capelli identities or properties of Schubert varieties or properties of Young bitableaux. Properties of leading monomials can be used to give new proofs of the Second Fundamental Theorems of vector covariants for  $GL(n, F)$  and  $O(n, F)$ ; such proofs are described in Section 6.

The list of references mentioned above is not meant to be exhaustive; more references can be found in the cited articles.

## 2. LEADING MONOMIALS

*Notation.* Let  $A = (a_{ij})$  denote an  $m \times n$  matrix of non-negative integers and let  $B = (b_{ij})$  denote a  $p \times n$  matrix of non-negative integers. Let  $C^A$  and  $X^B$  denote the monomials  $\prod_{1 \leq i \leq m} \prod_{1 \leq j \leq n} C_{ij}^{a_{ij}}$  and  $\prod_{1 \leq i \leq p} \prod_{1 \leq j \leq n} X_{ij}^{b_{ij}}$ , respectively. Define the exponent sequence of the monomial  $C^A X^B$  to be the sequence  $(a_{11}, a_{12}, \dots, a_{1n}, a_{21}, a_{22}, \dots, a_{mn}, b_{11}, b_{12}, \dots, b_{1n}, b_{21}, b_{22}, \dots, b_{pn})$ . If  $v$  and  $w$  are monomials in  $F[C, m \times n; X, p \times n]$ , let us write  $v < w$  if the exponent sequence of  $v$  is lexicographically less than the exponent sequence of  $w$ . Note that the relation  $<$  is a well-ordering of the monomials in  $F[C, m \times n; X, p \times n]$ .

Define the leading monomial of a non-zero element  $f$  of  $F[C, m \times n; X, p \times n]$  to be the biggest (with respect to the relation  $<$  defined above) monomial which appears in  $f$ .

Observe that, if  $M$  is a square submatrix of  $C_{m \times n}$  or of  $X_{p \times n}$ , then the

leading monomial of  $\det M$  is the product of the entries on the main diagonal of  $M$ . Observe also that if  $f$  and  $g$  are non-zero elements of  $F[C, m \times n; X, p \times n]$ , then the leading monomial of  $fg$  equals the product of the leading monomials of  $f$  and  $g$ .

**PROPOSITION 1.** *Let  $V$  and  $W$  be  $F$  vector subspaces of the algebra  $F[C, m \times n; X, p \times n]$ . Suppose that  $V \subseteq W$  and that the leading monomial of any element of  $W$  is also the leading monomial of an element of  $V$ ; then  $V = W$ .*

*Proof.* Let  $w$  be a non-zero element of  $W$ . By the hypothesis on the leading monomials of the elements of  $V$  and  $W$ , there is an element  $v$  in  $V$  which has the same leading monomial as  $w$ . Hence there is a scalar  $c$  such that either  $w - cv = 0$  or the leading monomial of  $w - cv$  is less than the leading monomial of  $w$ . Note also that if  $w$  does not lie in  $V$ , then  $w - cv$  does not lie in  $V$ . This argument shows that the set of leading monomials of elements of  $W - V$  does not have a minimum element. On the other hand, every non-empty set of monomials in  $F[C, m \times n; X, p \times n]$  has a minimum element. Therefore  $W - V$  is empty, so  $W = V$ . ■

*Notation.* Let  $A$  denote a  $k \times k$  matrix and let  $B$  denote an  $n \times n$  matrix; then  $A \oplus B$  denotes the  $(k + n) \times (k + n)$  matrix defined by

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0^T & B \end{pmatrix},$$

where  $0$  denotes a  $k \times n$  block of zeros.

Let  $I_k$  denote the  $k \times k$  identity matrix.

**DEFINITION.** Let  $s$ ,  $t$ , and  $n$  denote positive integers such that  $s \leq n$  and  $t \leq n$ . Let  $R_{st}$  denote the  $F$ -algebra homomorphism from  $F[C, m \times n; X, p \times n]$  to  $F[C, m \times 2; X, p \times 2]$  such that

$$R_{st} \left( \prod_{i,j} C_{ij}^{a_{ij}} \prod_{u,v} X_{uv}^{b_{uv}} \right) = \left( \prod_i C_{i1}^{a_{i1}} C_{i2}^{a_{i2}} \right) \left( \prod_u X_{u1}^{b_{u1}} X_{u2}^{b_{u2}} \right)$$

for all non-negative exponents  $a_{ij}$ ,  $b_{uv}$ . For example,

$$R_{23}(C_{11}^2 C_{31} C_{12}^3 C_{22}^4 C_{33}^5 C_{43} X_{21}^5 X_{13}^3) = C_{11}^3 C_{21}^4 C_{32}^5 C_{42} X_{12}^3.$$

**PROPOSITION 2.** *For every integer  $n \geq 1$ , let  $G(n)$  be a non-empty subset of  $GL(n, F)$ . Assume that, for all positive integers  $n$  and  $k$  and for all elements  $g$  in  $G(n)$ ,  $g \oplus I_k$  and  $I_k \oplus g$  lie in  $G(n + k)$ . If  $L$  is the leading monomial of a covariant of  $G(n)$ , where  $n \geq 2$ , then  $R_{t, t+1}(L)$  is the leading monomial of a covariant of  $G(2)$  for  $t = 1, 2, \dots, n - 1$ .*

*Proof.* Proceed by induction on  $n$ . When  $n = 2$ ,  $R_{12}$  is the identity map, so the proposition holds. Suppose now that  $n > 2$  and let  $f$  be a non-zero covariant of  $G(n)$ . One may write

$$f = \sum_A f_A A, \quad (2.1)$$

where the sum ranges over all monomials  $A$  in the letters  $C_{1n}, C_{2n}, \dots, C_{mn}, X_{1n}, X_{2n}, \dots, X_{pn}$  and where  $f_A$  lies in  $F[C, m \times (n-1); X, p \times (n-1)]$  for all  $A$ . Since  $f$  is a covariant of  $G(n)$ ,  $f^{g \oplus 1} = f$  for all  $g \in G(n-1)$ . Hence

$$\sum_A f_A A = \sum_A f_A^g A, \quad \text{for all } g \text{ in } G(n-1). \quad (2.2)$$

The monomials in the letters  $C_{1n}, C_{2n}, \dots, C_{mn}, X_{1n}, X_{2n}, \dots, X_{pn}$  form a basis for  $F[C, m \times n; X, p \times n]$  as a free  $F[C, m \times (n-1); X, p \times (n-1)]$ -module. Therefore Eq. (2.2) implies that  $f_A = f_A^g$  for all  $A$  and  $g$ , so

$$f_A \text{ is a covariant of } G(n-1), \quad \text{for all } A. \quad (2.3)$$

Let  $L$  denote the leading monomial of  $f$ . Equation (2.1) implies that there is a monomial  $B$  such that the leading monomial of  $f_B B$  equals  $L$ . Therefore, if  $1 \leq t \leq n-2$ , then  $R_{t, t+1}(L) = R_{t, t+1}$  (the leading monomial of  $f_B$ ). This equation, statement (2.3), and the induction hypothesis imply that

$$\text{when } 1 \leq t \leq n-2, \quad R_{t, t+1}(L) \text{ is the leading monomial of a covariant of } G(2). \quad (2.4)$$

Now write  $f = \sum_D h_D D$ , where the sum ranges over all monomials  $D$  in the letters  $C_{11}, C_{21}, \dots, C_{m1}, X_{11}, X_{21}, \dots, X_{p1}$  and where  $h_D \in F[C_{ij}, X_{kj}; 1 \leq i \leq m, 2 \leq j \leq n, 1 \leq k \leq p]$  for all  $D$ . Note that

$$h_D^{1 \oplus g} = h_D, \quad \text{for all } g \text{ in } G(n-1) \text{ and for all } D. \quad (2.5)$$

Note also that there is a monomial  $E$  in the letters  $C_{11}, \dots, C_{m1}, X_{11}, \dots, X_{p1}$  such that the leading monomial of  $h_E E$  equals the leading monomial of  $f$ . Therefore, if  $2 \leq t < n$ , then

$$R_{t, t+1}(L) = R_{t, t+1}(\text{the leading monomial of } h_E).$$

This equation, Eq. (2.5), and the induction hypothesis imply that if  $2 \leq t < n$ , then  $R_{t, t+1}(L)$  is the leading monomial of a covariant of  $G(2)$ . This statement and statement (2.4) establish the proposition. ■

*Notation.* If  $i$  and  $j$  are positive integers, define

$$\langle i|j \rangle_n = C_{i1}X_{j1} + C_{i2}X_{j2} + \cdots + C_{in}X_{jn}.$$

If  $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$  are positive integers, define  $\langle a_1, a_2, \dots, a_k | b_1, b_2, \dots, b_k \rangle_n$  to be the determinant of the  $k \times k$  matrix whose  $(i, j)$ th entry is  $\langle a_i | b_j \rangle_n$  for all  $i, j$ .

**PROPOSITION 3.** Let  $a_1, \dots, a_k, b_1, \dots, b_k$  be positive integers such that  $a_1 < a_2 < \cdots < a_k$  and  $b_1 < b_2 < \cdots < b_k$ . If  $n$  is an integer such that  $n < k$  then  $\langle a_1, \dots, a_k | b_1, \dots, b_k \rangle_n = 0$ . If  $k \leq n$  then the leading monomial of  $\langle a_1, \dots, a_k | b_1, \dots, b_k \rangle_n$  is  $C_{a_11}C_{a_22} \cdots C_{a_kk}X_{b_11}X_{b_22} \cdots X_{b_kk}$ .

*Proof.* Let  $G$  denote the  $k \times k$  matrix whose  $(i, j)$ th entry is  $\langle a_i | b_j \rangle_n$  for all  $i, j$ . Let  $A$  and  $B$  denote the  $k \times n$  matrices defined by

$$A = \begin{pmatrix} C_{a_11} & C_{a_12} & \cdots & C_{a_1n} \\ & & \ddots & \\ C_{a_k1} & C_{a_k2} & \cdots & C_{a_kn} \end{pmatrix}$$

and

$$B = \begin{pmatrix} X_{b_11} & X_{b_12} & \cdots & X_{b_1n} \\ & & \ddots & \\ X_{b_k1} & X_{b_k2} & \cdots & X_{b_kn} \end{pmatrix}.$$

Observe that

$$G = A B^T. \quad (2.6)$$

If  $S$  is a subset of  $\{1, 2, \dots, n\}$  of size  $k$ , define  $A_S$  to be the  $k \times k$  submatrix of  $A$  whose columns are indexed by the elements of  $S$  and define  $B_S$  to be the analogous submatrix of  $B$ . Applying the Binet–Cauchy formula [9, p. 9] to Eq. (2.6) yields

$$\det G = \sum_{\substack{S \subseteq \{1, \dots, n\} \\ |S| = k}} \det A_S \det B_S. \quad (2.7)$$

Note that when  $k > n$ , the preceding sum is empty, so  $\det G = 0$ . Therefore  $\langle a_1, \dots, a_k | b_1, \dots, b_k \rangle_n$  equals zero when  $k > n$ . Suppose now that  $k \leq n$ . Set  $S' = \{1, 2, \dots, k\}$  and observe that if  $S$  is a  $k$ -subset of  $\{1, 2, \dots, n\}$  which is different than  $S'$ , then the leading monomial of  $\det A_S \det B_S$  is strictly greater than the leading monomial of  $\det A_{S'} \det B_{S'}$ . Therefore the leading monomial of  $\sum_S \det A_S \det B_S$  equals the leading monomial of  $\det A_{S'}$

$\det B_{S'}$ , which equals  $C_{a_{11}} C_{a_{22}} \cdots C_{a_{kk}} X_{b_{11}} X_{b_{22}} \cdots X_{b_{kk}}$ . This statement and Eq. (2.7) imply that the leading monomial of  $\langle a_1, \dots, a_k | b_1, \dots, b_k \rangle_n$  is  $C_{a_{11}} \cdots C_{a_{kk}} X_{b_{11}} \cdots X_{b_{kk}}$ . ■

PROPOSITION 4. *Set*

$$S(n) = \{g: g \text{ is an } n \times n \text{ minor of } C_{m \times n} \text{ or an } n \times n \text{ minor of } X_{p \times n} \\ \text{or, for some integer } k \text{ satisfying } 1 \leq k < n, \text{ a } k \times k \text{ minor} \\ \text{of } C_{m \times n} X_{p \times n}^T\}.$$

Let  $L$  be a monomial in  $F[C, m \times n; X, p \times n]$ , where  $n \geq 2$ . Suppose that  $R_{t+1}(L)$  is the leading monomial of a product of elements of  $S(2)$  for  $t = 1, 2, \dots, n-1$ ; then  $L$  is the leading monomial of a product of elements of  $S(n)$ .

*Proof.* Proceed by induction on  $n$ . When  $n = 2$ ,  $R_{12}$  is the identity map, so the proposition holds. Suppose now that  $n > 2$ . Let  $L'$  denote the monomial which is obtained from  $L$  by replacing each of the letters  $C_{1n}, C_{2n}, \dots, C_{mn}, X_{1n}, X_{2n}, \dots, X_{pn}$  by ones. The induction hypothesis implies that  $L'$  is the leading monomial of a product of elements of  $S(n-1)$ . Therefore there are polynomials  $g_1, g_2$ , and  $g_3$  such that  $g_1$  is a product of  $(n-1) \times (n-1)$  minors of  $C_{m \times (n-1)}$ ,  $g_2$  is a product of  $(n-1) \times (n-1)$  minors of  $X_{p \times (n-1)}$ ,  $g_3$  is a product of minors of  $C_{m \times (n-1)} X_{p \times (n-1)}^T$  of order less than  $n-1$ , and

$$\text{the leading monomial of } g_1 g_2 g_3 \text{ is } L'. \quad (2.8)$$

If  $q, r, \dots, w$  are  $k$  positive integers, define

$$C[q \, r \, \dots \, w] = \det \begin{pmatrix} C_{q1} & C_{q2} & \cdots & C_{qk} \\ C_{r1} & C_{r2} & \cdots & C_{rk} \\ & & \ddots & \\ C_{w1} & C_{w2} & \cdots & C_{wk} \end{pmatrix}$$

and

$$X[q \, r \, \dots \, w] = \det \begin{pmatrix} X_{q1} & X_{q2} & \cdots & X_{qk} \\ X_{r1} & X_{r2} & \cdots & X_{rk} \\ & & \ddots & \\ X_{w1} & X_{w2} & \cdots & X_{wk} \end{pmatrix}.$$

One may write

$$g_1 = \prod_{1 \leq i \leq u} C[a_{i1} a_{i2} \cdots a_{i(n-1)}] \quad (2.9)$$

and

$$g_2 = \prod_{1 \leq i \leq v} X[b_{i1} b_{i2} \cdots b_{in-1}], \quad (2.10)$$

where  $a_{i1} < a_{i2} < \cdots < a_{in-1}$  and  $b_{k1} < b_{k2} < \cdots < b_{kn-1}$  for all  $i, k$ . Equations (2.8), (2.9), and (2.10) imply that, if one sets  $a(i) = a_{in-1}$  and  $b(j) = b_{jn-1}$  for all  $i$  and  $j$ , then  $(\prod_i C_{a(i)n-1})(\prod_j X_{b(j)n-1})$  is the biggest divisor of  $L$  which lies in  $F[C_{in-1}, X_{jn-1}; 1 \leq i \leq m, 1 \leq j \leq p]$ . Recall also that  $R_{n-1n}(L)$  is the leading monomial of a product of elements of  $S(2)$ . Therefore one may, after permuting the first subscripts of the  $a_{ij}$ 's and  $b_{ij}$ 's, express  $R_{n-1n}(L)$  as

$$\begin{aligned} R_{n-1n}(L) = & \text{the leading monomial of } \prod_{1 \leq i \leq u-w} C[a_{in-1} a_{in}] \\ & \cdot \prod_{1 \leq i \leq v-w} X[b_{in-1} b_{in}] \cdot \prod_{1-w \leq i \leq 0} \langle a_{u+i n-1} | b_{v+i n-1} \rangle_2, \end{aligned} \quad (2.11)$$

where  $w$  is an integer satisfying  $0 \leq w \leq \text{minimum}\{u, v\}$  and the integers  $a_{in}, b_{kn}$  satisfy the conditions

$$a_{in-1} < a_{in} \quad \text{and} \quad b_{kn-1} < b_{kn}, \quad \text{for all } i \text{ and } k. \quad (2.12)$$

Statements (2.8)–(2.12) imply that

$$\begin{aligned} L \text{ is the leading monomial of } & \prod_{1 \leq i \leq u-w} C[a_{i1} a_{i2} \cdots a_{in}] \\ & \cdot \prod_{1 \leq i \leq v-w} X[b_{i1} b_{i2} \cdots b_{in}] \cdot \prod_{1-w \leq i \leq 0} C[a_{u+i1} a_{u+i2} \cdots a_{u+in-1}] \\ & \cdot \prod_{1-w \leq i \leq 0} X[b_{v+i1} b_{v+i2} \cdots b_{v+in-1}] \cdot g_3. \end{aligned} \quad (2.13)$$

Proposition 3 implies that the leading monomial of  $C[a_{j1} a_{j2} \cdots a_{jn-1}] \cdot X[b_{k1} b_{k2} \cdots b_{kn-1}]$  equals the leading monomial of  $\langle a_{j1}, a_{j2}, \dots, a_{jn-1} | b_{k1}, b_{k2}, \dots, b_{kn-1} \rangle_n$ . Proposition 3 also implies that if  $1 \leq t \leq n-1$ , then the leading monomial of a  $t \times t$  minor of  $C_{m \times (n-1)} X_{p \times (n-1)}^T$  is the same as the leading monomial of the analogous minor of  $C_{m \times n} X_{p \times n}^T$ . Therefore the leading monomial of  $g_3$  equals the leading monomial of a product of minors of  $C_{m \times n} X_{p \times n}^T$ . These observations and statement (2.13) imply that  $L$  is the leading monomial of a product of elements of  $S(n)$ . ■



### 3. COVARIANTS OF THE GROUP OF UNIMODULAR UPPER TRIANGULAR MATRICES

If  $M$  denotes an  $n \times n$  submatrix of  $C_{m \times n}$ , then

$$(\det M)^g = \det(Mg) = (\det M)(\det g), \quad \text{for every } g \in GL(n, F). \quad (3.1)$$

If  $W$  denotes an  $n \times n$  submatrix of  $X_{p \times n}$ , then

$$(\det W)^{g^*} = \det(W(g^{-1})^T) = (\det W)(\det g)^{-1}, \quad \text{for every } g \in GL(n, F). \quad (3.2)$$

Equations (3.1) and (3.2) imply that

$$\text{every } n \times n \text{ minor of } C_{m \times n} \text{ and every } n \times n \text{ minor of } X_{p \times n} \text{ is a} \\ \text{covariant of } SL(n, F). \quad (3.3)$$

Observe that, that for every element  $g$  in  $GL(n, F)$ ,

$$\begin{aligned} (C_{i1}X_{j1} + C_{i2}X_{j2} + \cdots + C_{in}X_{jn})^g \\ = (C_{i1}C_{i2} \cdots C_{in})g[(X_{j1}X_{j2} \cdots X_{jn})(g^{-1})^T]^T \\ = C_{i1}X_{j1} + C_{i2}X_{j2} + \cdots + C_{in}X_{jn}. \end{aligned}$$

Hence

$$\langle i|j \rangle_n \text{ is a covariant of } GL(n, F), \quad \text{for all } i, j. \quad (3.4)$$

Let  $H$  denote a  $k \times n$  matrix whose entries lie in a commutative ring.

**DEFINITION.** An  $H$ -matrix is a matrix with  $n$  columns whose entries are rows of  $H$ .

If  $M$  denotes an  $H$ -matrix, e.g.,

$$M = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \\ & & \vdots & \\ r_1 & r_2 & \cdots & r_n \end{pmatrix},$$

then let  $|M|$  denote the product

$$\det \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \det \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \cdots \det \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix}.$$

The element  $|M|$  is called the value of  $M$ . For example, if

$$M = \begin{pmatrix} (u & v)(x & y) \\ (u & v)(0 & 1) \end{pmatrix},$$

then its value is  $(uy - vx)u$ .

Note that if each row of  $M$  has distinct entries, then  $|M|$  is a certain product of  $n \times n$  minors of  $H$ .

The empty set is also considered to be an  $H$ -matrix, and its value is defined to be 1.

**DEFINITION.** Assume that  $H$  has distinct rows, and order the rows of  $H$  from top to bottom. An  $H$ -matrix  $M$  is said to be standard if the entries in each row of  $M$  are strictly increasing from left to right and the entries in each column are weakly increasing (i.e., non-decreasing) from top to bottom.

The notion of a standard matrix is due to A. Young [22].

The values of standard  $H$ -matrices are called standard products of  $n \times n$  minors of  $H$ .

**DEFINITION.** An  $SL(2)$ -triple is a triple  $(A, B, D)$  which satisfies the following three conditions.

- (i)  $A$  is a  $C_{m \times 2}$ -matrix.
- (ii)  $B$  is an  $X_{p \times 2}$ -matrix.
- (iii)  $D$  is a  $(C_{X_{p \times 2}}^{m \times 2})$ -matrix such that every entry of the first column of  $D$  is a row of  $C_{m \times 2}$  and every entry of the second column of  $D$  is a row of  $X_{p \times 2}$ .

*Notation.* Suppose that

$$D = \begin{pmatrix} a_1 & b_1 \\ \vdots & \vdots \\ a_t & b_t \end{pmatrix},$$

where  $a_1, \dots, a_t$  and  $b_1, \dots, b_t$  are  $n$ -component row vectors. Let  $\langle D \rangle$  denote the product  $(a_1 b_1^T) \cdots (a_t b_t^T)$ . If  $D$  is the empty set, then  $\langle D \rangle$  is defined to be 1.

**DEFINITION.** The value of an  $SL(2)$ -triple  $(A, B, D)$  is defined to be the product  $|A| |B| \langle D \rangle$ .

**DEFINITION.** An  $SL(2)$ -triple  $(A, B, D)$  is said to be standard if  $A$ ,  $B$ , and  $D$  are standard, every entry of the first column of  $A$  is less than or equal to every entry of the first column of  $D$ , and every entry of the first column of  $B$  is less than or equal to every entry of the second column of  $D$ .

**PROPOSITION 5.** *If  $(A, B, D)$  is an  $SL(2)$ -triple, then  $|A| |B| \langle D \rangle$  lies in the additive group generated by the values of standard  $SL(2)$ -triples.*

In the case that  $B$  and  $D$  are empty, the proposition is a special case of a result of Hodge [14]. A nice proof of this case is given by Kung and Rota in [16, Lemma 3.2, p. 36]. The proof of Kung and Rota can be easily modified to give a proof of Proposition 5. The details are omitted.

**COROLLARY.** *Let  $M$  be a  $k \times 2$  matrix whose rows are distinct and whose entries lie in a commutative ring. Every product of  $2 \times 2$  minors of  $M$  lies in the additive group generated by standard products of  $2 \times 2$  minors of  $M$ .*

*Proof.* By considering a homomorphism which maps a set of indeterminates to the entries of  $M$ , one may reduce to the case that  $M = C_{m \times 2}$ . In this case the corollary is proved in [14; 16, Lemma 3.2, p. 36]. The corollary also follows in this case from Proposition 5, with  $B$  and  $D$  being empty and the letters  $X_{ij}$  being replaced with zeros. ■

As in Section 2, let  $I_2$  denote the  $2 \times 2$  identity matrix. Let  $e_1$  and  $e_2$  denote the first and second rows, respectively, of  $I_2$ .

If  $T$  denotes a  $(C_{n \times 2}^{I_2})$ -matrix, let  $e_1(T)$  and  $e_2(T)$  denote the number of appearances of  $e_1$  and  $e_2$ , respectively, as entries of  $T$ .

**PROPOSITION 6.** *Let  $T_1$  and  $T_2$  be standard  $(C_{n \times 2}^{I_2})$ -matrices such that  $e_1(T_1) = e_1(T_2) = 0$ . If the leading monomial of  $|T_1|$  equals the leading monomial of  $|T_2|$ , then  $T_1 = T_2$ .*

*Proof.* Let  $w$  denote the leading monomial of  $|T_1|$ . Note that, since  $e_1(T_1) = 0$  and the entries in every row of  $T_1$  are strictly increasing, the number of appearances of  $(C_{i1} \ C_{i2})$  in the first column of  $T_1$  equals the exponent of  $C_{i1}$  in  $w$  and the number of appearances of  $(C_{i1} \ C_{i2})$  in the second column of  $T_1$  equals the exponent of  $C_{i2}$  in  $w$ . Therefore the matrix  $T_1$  is uniquely determined by  $w$ . This establishes the proposition. ■

*Remark.* If  $f$  is a non-zero element of  $F[C, m \times n]$ , define the trailing monomial of  $f$  to be the smallest monomial which appears in  $f$ . Let  $T_1$  and  $T_2$  be standard  $(C_{n \times 2}^{I_2})$ -matrices such that  $e_2(T_1) = e_2(T_2) = 0$ . By an argument similar to the one used in the proof of Proposition 6, one can show that if  $|T_1|$  and  $|T_2|$  have the same trailing monomials, then  $T_1 = T_2$ .

Let  $SUT(n, F)$  denote the set of upper triangular matrices in  $SL(n, F)$

and let  $UUT(n, F)$  denote the set of unipotent upper triangular matrices in  $SL(n, F)$ , i.e.,

$$UTT(n, F) = \{B \in SUT(n, F) : \text{every entry on the main diagonal of } B \text{ equals } 1\}.$$

Recall that  $F$  denotes an infinite field.

**PROPOSITION 7.** (i) *Every invariant of  $UUT(2, F)$  in  $F[C, m \times 2]$  is a linear combination of standard products of  $2 \times 2$  minors of  $\begin{pmatrix} C_{m \times 2} \\ 0 \end{pmatrix}$ .*

(ii) *Every invariant of  $SUT(2, F)$  in  $F[C, m \times 2]$  is a linear combination of standard products of  $2 \times 2$  minors of  $C_{m \times 2}$ .*

*Proof.* Let  $H = \begin{pmatrix} C_{m \times 2} \\ 0 \end{pmatrix}$ . Observe that, if  $1 \leq i \leq m$ , then the elements  $C_{i1}$  and  $-C_{i2}$  are  $2 \times 2$  minors of  $H$ . Therefore every monomial in  $F[C, m \times 2]$  is a scalar multiple of a product of  $2 \times 2$  minors of  $H$ . This observation and the corollary to Proposition 5 imply that, for every non-zero element  $f$  in  $F[C, m \times 2]$ , there are non-zero scalars  $c_1, c_2, \dots, c_k$  and distinct standard  $H$ -matrices  $A_1, A_2, \dots, A_k$  such that

$$f = c_1 |A_1| + \dots + c_k |A_k|. \quad (3.5)$$

Assume furthermore that the row  $(e_1 e_2)$  does not appear in any of the matrices  $A_1, \dots, A_k$ ; this assumption does not entail any loss of generality because the deletion of all appearances of the row  $(e_1 e_2)$  in  $A_1, \dots, A_k$  does not affect the polynomials  $|A_1|, \dots, |A_k|$ . Note that

$$\text{for every subscript } i, \text{ the first column of } A_i \text{ does not contain } e_1 \text{ or } e_2, \quad (3.6)$$

because  $A_i$  is standard and does not contain the row  $(e_1 e_2)$ .

Assume now that  $f$  is an invariant of  $UUT(2, F)$ . It will be shown that  $e_1(A_i) = 0$  for all  $i$ . Set  $g(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ . Let  $r_i = (C_{i1} \ C_{i2})$  and observe that, for all  $t \in F$ ,

$$|r_i r_j|^{g(t)} = |r_i r_j|, \quad (3.7)$$

$$|r_i e_2|^{g(t)} = C_{i1}^{g(t)} = |r_i e_2|, \quad (3.8)$$

and

$$\begin{aligned} |r_i e_1|^{g(t)} &= -C_{i2}^{g(t)} \\ &= -(C_{i2} + t C_{i1}) \\ &= |r_i e_1| - t |r_i e_2|. \end{aligned} \quad (3.9)$$

For  $i = 1, 2, \dots, k$ , let  $e(i) = e_1(A_i)$  and let  $\hat{A}_i$  denote the matrix which is obtained from  $A_i$  by replacing every appearance of the element  $e_1$  with the element  $e_2$ . Let  $T$  be an indeterminate. Statements (3.6)–(3.9) imply that

$$\text{if } e(i) > 0 \text{ then } |A_i|^{g(T)} - (-T)^{e(i)} |\hat{A}_i| \text{ lies in} \\ F[C, m \times 2] + T F[C, m \times 2] + \dots + T^{e(i)-1} F[C, m \times 2] \quad (3.10)$$

and

$$\text{if } e(i) = 0 \text{ then } |A_i|^{g(T)} = |A_i| = |\hat{A}_i|. \quad (3.11)$$

Let  $E = \max\{e(1), e(2), \dots, e(k)\}$  and let  $J = \{j: e(j) = E\}$ . Write

$$f^{g(T)} = f_0 + f_1 T + \dots + f_r T^r,$$

where  $f_j$  lies in  $F[C, m \times 2]$  for all  $j$ . Statements (3.5), (3.10), and (3.11) imply that

$$f_E = (-1)^E \sum_{j \in J} c_j |\hat{A}_j|. \quad (3.12)$$

Statement (3.6) and the hypothesis that  $A_1, \dots, A_k$  are distinct standard matrices imply that the elements  $\hat{A}_j$ , for  $j$  in  $J$ , are distinct standard matrices. Therefore Proposition 6 implies that the elements  $|\hat{A}_j|$ , for  $j$  in  $J$ , have distinct leading monomials. Hence these elements are linearly independent, so Eq. (3.12) implies that  $f_E \neq 0$ . On the other hand, since  $f$  is an invariant of  $UUT(2, F)$  and  $F$  is infinite,  $f_j = 0$  for all  $j > 0$ . Therefore  $E = 0$ . This shows that  $e_1(A_i) = 0$  for all  $i$  and hence establishes statement (i) of the proposition.

Suppose now that  $f$  is an invariant of  $SUT(2, F)$ . Set  $h(t) = \begin{pmatrix} t & 0 \\ 0 & 1/t \end{pmatrix}$  and note that  $f = f^{h(t)}$  for all  $t \neq 0$  in  $F$ . Equation (3.5) and the fact that  $e_1(A_i) = 0$  for all  $i$  imply that

$$f = f^{h(t)} = \sum_i c_i t^{e_2(A_i)} |A_i|, \quad \text{for all } t \neq 0 \text{ in } F. \quad (3.13)$$

Since a polynomial with infinitely many roots must be identically zero, the right side of Eq. (3.13) must equal  $f$  for all elements  $t$  in  $F$ . Setting  $t = 0$ , Eq. (3.13) yields an expression for  $f$  as a linear combination of standard products of  $2 \times 2$  minors of  $C_{m \times 2}$ . ■

**PROPOSITION 8.** *Every covariant of  $SUT(2, F)$  is a linear combination of values of standard  $SL(2)$ -triples.*

*Proof.* The key idea can be found in [21, p. 49] but is repeated here for the convenience of the reader. Set

$$M = \begin{pmatrix} C_{11} & C_{12} \\ & \vdots \\ C_{m1} & C_{m2} \\ -X_{12} & X_{11} \\ & \vdots \\ -X_{p2} & X_{p1} \end{pmatrix}.$$

Note that

$$(-X_{i2}^* X_{i1}^{g*}) = (-X_{i2} X_{i1}) g, \quad (3.14)$$

for all  $g \in SL(2, F)$  and all positive integers  $i$ .

Let  $h$  denote the  $F$ -algebra homomorphism from  $F[C, (m+p) \times 2]$  to  $F[C, m \times 2; X, p \times 2]$  such that

$$\begin{pmatrix} h(C_{11}) & h(C_{12}) \\ & \vdots \\ h(C_{m+p1}) & h(C_{m+p2}) \end{pmatrix} = M.$$

Let  $f \in F[C, (m+p) \times 2]$ . Equation (3.14) implies that  $h(f)$  is a covariant of  $SUT(2, F)$  if and only if  $f$  is an invariant of  $SUT(2, F)$ . This observation and Proposition 7 imply that every covariant of  $SUT(2, F)$  in  $F[C, m \times 2; X, p \times 2]$  is a linear combination of products of  $2 \times 2$  minors of  $M$ . Such products are values of  $SL(2)$ -triples, so Proposition 5 implies that every covariant of  $SUT(2, F)$  is a linear combination of values of standard  $SL(2)$ -triples. ■

**PROPOSITION 9.** *The set of covariants of  $SUT(n, F)$  in  $F[C, m \times n; X, p \times n]$  is generated as an  $F$ -algebra by the set  $\{h: h \text{ is an } n \times n \text{ minor of } C_{m \times n} \text{ or an } n \times n \text{ minor of } X_{p \times n} \text{ or an element of the form } \langle i|j \rangle_n\}$ .*

*Proof.* Define  $S(n)$  as in Proposition 4 and let  $L'_n$  denote the set of leading monomials of products of elements of  $S(n)$ . Let  $L_n$  denote the set of leading monomials of covariants of  $SUT(n, F)$  in  $F[C, m \times n; X, p \times n]$ . It will be shown that  $L_n = L'_n$  for all  $n$ . Statements (3.3) and (3.4) imply that every element of  $S(n)$  is a covariant of  $SUT(n, F)$ .

Note that the values of distinct standard  $SL(2)$ -triples have distinct leading monomials. This observation and Proposition 8 imply that

$$L_2 \subseteq L'_2. \quad (3.15)$$

Suppose now that  $n > 2$  and let  $w$  denote an element of  $L_n$ . Proposition 2 and relation (3.15) imply that

$$R_{t, t+1}(w) \in L_2 \subseteq L'_2, \quad \text{for } t = 1, 2, \dots, n-1.$$

This relation and Proposition 4 imply that  $w \in L'_n$ . Thus

$$L_n \subseteq L'_n. \quad (3.16)$$

This containment and Proposition 1 imply that the set of covariants of  $SUT(n, F)$  equals the vector space spanned by  $S(n)$ . ■

*Remarks.* Proposition 9 and statements (3.3) and (3.4) imply that the covariants of  $SL(n, F)$  are the same as those of  $SUT(n, F)$ . Let  $SLT(n, F)$  denote the set of lower triangular matrices in  $SL(n, F)$ . The remark following Proposition 6 and the proofs of Propositions 7, 8, and 9 imply that the covariants of  $SLT(n, F)$  are also the same as those of  $SUT(n, F)$ .

One can deduce from Proposition 9 that the set of covariants of the group of upper triangular matrices in  $GL(n, F)$  is generated as an  $F$ -algebra by the elements of the form  $\langle i|j \rangle_n$ . The details of the proof can be found, for example, in [19, pp. 25–26].

#### 4. INVARIANTS OF THE SPECIAL ORTHOGONAL GROUP OVER AN INFINITE FIELD OF CHARACTERISTIC DIFFERENT FROM TWO

*Notation.* Let  $C\langle i|j \rangle_n$  denote the polynomial  $C_{i1}C_{j1} + C_{i2}C_{j2} + \dots + C_{in}C_{jn}$ . Let  $C\langle a_1, a_2, \dots, a_k | b_1, b_2, \dots, b_k \rangle_n$  denote the determinant of the  $k \times k$  matrix whose  $(i, j)$ th entry is  $C\langle a_i | b_j \rangle_n$  for all  $i, j$ .

Observe that, if  $r_i$  denotes the  $i$ th row of  $C_{m \times n}$  and  $g \in GL(n, F)$ , then

$$(r_i r_j^T)^g = (r_i g)(r_j g)^T = r_i g g^T r_j^T.$$

Therefore

$$C\langle i|j \rangle_n \text{ is an invariant of } O(n, F), \quad \text{for all } i, j. \quad (4.1)$$

**PROPOSITION 10.** Let  $a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k$  denote positive integers such that  $a_1 < a_2 < \dots < a_k$  and  $b_1 < b_2 < \dots < b_k$ . If  $n$  is an integer such that  $n < k$ , then  $C\langle a_1, \dots, a_k | b_1, \dots, b_k \rangle_n = 0$ . If  $b \geq k$  then the leading monomial of  $C\langle a_1, \dots, a_k | b_1, \dots, b_k \rangle_n$  is  $C_{a_1 1} C_{a_2 2} \dots C_{a_k k} C_{b_1 1} C_{b_2 2} \dots C_{b_k k}$ .

*Proof.* Let  $h$  denote the  $F$ -algebra homomorphism from  $F[C, m \times n; X, m \times n]$  to  $F[C, m \times n]$  such that  $h(C_{ij}) = C_{ij}$  and  $h(X_{ij}) = C_{ij}$  for all  $i, j$ . The proposition may be established by applying  $h$  to both sides of Eqs. (2.6) and (2.7) and using the argument in the proof of Proposition 3. ■

**DEFINITION.** An  $SO(2)$ -tableau is a pair  $(M, W)$  such that  $M$  is a  $(C_{m \times 2}^{I_2})$ -matrix,  $W$  is a sequence of rows of  $C_{m \times 2}$ , and  $W$  has an even number of terms.

An  $SO(2)$ -tableau  $(M, W)$  is said to be standard if the following conditions hold.

- (i)  $M$  is standard.
- (ii) Every entry in the first column of  $M$  is a row of  $C_{m \times 2}$  and the row  $(1 \ 0)$  appears at most once as an entry of  $M$ .
- (iii) The sequence  $W$  is weakly increasing, and every term in  $W$  is greater than or equal to every entry in the first column of  $M$ .

*Notation.* Let  $(M, W)$  be an  $SO(2)$ -tableau. If  $W$  is empty, define  $\langle W \rangle = 1$ , and if  $W = (r_1, r_2, \dots, r_{2t})$ , define  $\langle W \rangle = (r_1 r_2^T) \cdots (r_{2t-1} r_{2t}^T)$ . The expression  $\langle r_1, r_2, \dots, r_{2t} \rangle$  also denotes the product  $(r_1 r_2^T) \cdots (r_{2t-1} r_{2t}^T)$ .

Define  $|M|$  as in Section 3. The value of  $(M, W)$  is defined to be  $|M| \langle W \rangle$ .

**PROPOSITION 11.** *The value of every  $SO(2)$ -tableau lies in the additive group generated by the values of standard  $SO(2)$ -tableaux.*

*Proof.* As in Section 3, let  $e_1$  and  $e_2$  denote the first and second rows, respectively, of  $I_2$ . If  $r$  and  $s$  denote rows of  $C_{m \times 2}$ , then

$$|s \ r| = -|r \ s|,$$

$$\begin{vmatrix} r & e_1 \\ s & e_1 \end{vmatrix} = \langle r, s \rangle - \begin{vmatrix} r & e_2 \\ s & e_2 \end{vmatrix},$$

and

$$|e_1 e_2| = \det I_2 = 1.$$

By repeatedly applying these identities, one can express the value of any  $SO(2)$ -tableau as an element of the additive group generated by the values of  $SO(2)$ -tableaux  $(M, W)$  which satisfy the following conditions.

The entries in every row of  $M$  are strictly increasing. (4.2)

The element  $e_1$  appears at most once as an entry of  $M$ . (4.3)

The row  $(e_1 e_2)$  does not appear in  $M$ . (4.4)

Let  $T$  denote the set of  $SO(2)$ -tableaux which satisfy conditions (4.2), (4.3), and (4.4). Note that every element of  $T$  satisfies condition (ii) of the definition of standard  $SO(2)$ -tableaux.



Let  $(M, W)$  denote an  $SO(2)$ -tableau, and write

$$M = \begin{pmatrix} a_1 & b_1 \\ \vdots & \vdots \\ a_t & b_t \end{pmatrix} \quad \text{and} \quad W = (w_1, w_2, \dots, w_{2u}).$$

Define the row-sequence of  $(M, W)$  to be the sequence  $(a_1, b_1, a_2, b_2, \dots, a_t, b_t, w_1, w_2, \dots, w_{2u})$ . If  $(L, V)$  is another  $SO(2)$ -tableau, let us write  $(L, V) < (M, W)$  if the row-sequence of  $(L, V)$  is lexicographically less than the row-sequence of  $(M, W)$ . Let  $\hat{M}$  denote the matrix which is obtained from  $M$  by replacing every appearance of the entry  $e_1$  with the entry  $e_2$ . Define  $p(M, W)$  to be the set of elements  $(L, V)$  in  $T$  such that

- (i) the row-sequence of  $(\hat{L}, V)$  is a permutation of a subsequence of the row-sequence of  $(\hat{M}, W)$  and
- (ii) either  $(L, V) < (M, W)$  or the row-sequence of  $(L, V)$  equals the row-sequence of  $(M, W)$  and  $V$  has fewer terms than  $W$  or the row-sequence of  $(L, V)$  has fewer terms than the row-sequence of  $(M, W)$ .

Let  $(M, W)$  denote an element of  $T$ . It will be shown that either  $(M, W)$  is standard or  $|M| \langle W \rangle$  lies in the additive group generated by the values of standard  $SO(2)$ -tableaux in  $p(M, W)$ .

After permuting the rows of  $M$ , one may assume that the entries in the first column of  $M$  are weakly increasing. This assumption and the equation

$$\begin{vmatrix} a & d \\ b & c \end{vmatrix} = \begin{vmatrix} a & c \\ b & d \end{vmatrix} - \begin{vmatrix} a & b \\ c & d \end{vmatrix}$$

imply that if  $M$  is not standard, then one can write  $|M| = |L_1| - |L_2|$ , where  $(L_1, W)$  and  $(L_2, W)$  lie in  $p(M, W)$ .

Now let  $a, b, c$ , and  $d$  denote entries of  $W$  and observe that

$$\begin{aligned} \langle b, a \rangle &= \langle a, b \rangle, \\ \langle c, d, a, b \rangle &= \langle a, b, c, d \rangle, \end{aligned}$$

and

$$\langle a, c, b, d \rangle = \langle a, b, c, d \rangle - \begin{vmatrix} a & d \\ b & c \end{vmatrix}.$$

The preceding equations imply that if  $W$  is not weakly increasing, then  $|M| \langle W \rangle$  is in the additive group generated by the values of elements of  $p(M, W)$ .

Suppose now that some element in  $W$  is strictly less than some element in the first column of  $M$ . Note that, if  $a, b, c$ , and  $d$  are rows of  $C_{m \times 2}$  then

$$|c \ d| \langle a, b \rangle = -|a \ c| \langle b, d \rangle + |a \ d| \langle b, c \rangle$$

and

$$|c \ e_2| \langle a, b \rangle = \begin{vmatrix} a & c \\ b & e_1 \end{vmatrix} + |a \ e_2| \langle b, c \rangle.$$

Therefore, if  $e_1$  does not appear in  $M$ , then there are elements  $(L_1, V_1)$  and  $(L_2, V_2)$  in  $p(M, W)$  such that  $|M| \langle W \rangle = |L_1| \langle V_1 \rangle \pm |L_2| \langle V_2 \rangle$ . Note also that

$$|c \ e_1| \langle a, b \rangle = - \begin{vmatrix} a & c \\ b & e_2 \end{vmatrix} + |a \ e_1| \langle b, c \rangle$$

and

$$\begin{vmatrix} a & e_1 \\ d & e_2 \end{vmatrix} \langle b, c \rangle = - \begin{vmatrix} a & e_2 \\ b & d \end{vmatrix} + |b \ d| \langle a, c \rangle + \begin{vmatrix} a & e_1 \\ b & e_2 \end{vmatrix} \langle c, d \rangle.$$

Therefore, if  $e_1$  does appear in  $M$ , then  $|M| \langle W \rangle$  is in the additive group generated by the values of elements of  $p(M, W)$ .

The preceding observations imply that if  $(M, W)$  is not standard, then  $|M| \langle W \rangle$  can be expressed as a linear combination, with integer coefficients, of values of elements  $(L_i, V_i)$  in  $p(M, W)$ . If  $(L_i, V_i)$  is not standard for some  $i$ , then  $|L_i| \langle V_i \rangle$  can be expressed as a linear combination, with integer coefficients, of values of elements in  $p(L_i, V_i)$ . Note that  $p(M, W)$  is finite and, for every element  $(L, V)$  in  $p(M, W)$ ,  $p(L, V)$  is a proper subset of  $p(M, W)$ . Therefore by iterating this process one eventually obtains an expression for  $|M| \langle W \rangle$  as a linear combination of values of standard  $SO(2)$ -tableaux. ■

**PROPOSITION 12.** *Let  $(L, V)$  and  $(M, W)$  denote standard  $SO(2)$ -tableaux such that  $e_1(L) = e_1(M) = 0$  and  $e_2(L) = e_2(M)$ . If the leading monomial of  $|L| \langle V \rangle$  equals the leading monomial of  $|M| \langle W \rangle$ , then  $(L, V) = (M, W)$ .*

*Proof.* Suppose that the leading monomial of  $|M| \langle W \rangle$  is  $\prod_{1 \leq i \leq t} C_{a(i)1} \prod_{1 \leq j \leq u} C_{b(j)2}$ , where  $a(1) \leq a(2) \leq \dots \leq a(t)$  and  $b(1) \leq b(2) \leq \dots \leq b(u)$ . Let  $A(i)$  denote the  $a(i)$ th row of  $C_{m \times 2}$

and let  $B(j)$  denote the  $b(j)$ th row of  $C_{m \times 2}$  for all  $i, j$ . Note that, since  $e_1(M) = 0$  and  $M$  is standard, the second column of  $M$  equals  $(B(1)B(2) \cdots B(u)e_2 \cdots e_2)^T$ , with the entry  $e_2$  appearing  $e_2(M)$  times. Note also that the first column of  $M$  must equal  $(A(1)A(2) \cdots A(u + e_2(M)))^T$  and  $W$  must equal  $(A(u + e_2(M) + 1), A(u + e_2(M) + 2), \dots, A(t))$ . Thus  $(M, W)$  is uniquely determined by  $e_2(M)$  and the leading monomial of  $|M| \langle W \rangle$ . This establishes the proposition. ■

**PROPOSITION 13.** *Let  $F$  denote an infinite field of characteristic different from two. Every invariant of  $SO(2, F)$  is a linear combination of values of standard  $SO(2)$ -tableaux  $(M, W)$  such that  $e_1(M) = e_2(M) = 0$ .*

*Proof.* Let  $f$  denote a non-zero invariant of  $SO(2, F)$  in  $F[C, m \times 2]$ . Note that every monomial in  $F[C, m \times 2]$  can be expressed as the value of a certain  $SO(2)$ -tableau. This remark and Proposition 11 imply that the values of standard  $SO(2)$ -tableaux span  $F[C, m \times 2]$ . Therefore there are distinct standard  $SO(2)$ -tableaux  $(M_1, W_1), \dots, (M_k, W_k)$  and non-zero scalars  $c_1, \dots, c_k$  such that

$$f = c_1 |M_1| \langle W_1 \rangle + \cdots + c_k |M_k| \langle W_k \rangle. \quad (4.5)$$

To finish the proof, it suffices to show that  $e_1(M_i) = e_2(M_i) = 0$  for all  $i$ .

Set

$$g(t) = \frac{1}{t^2 + 1} \begin{pmatrix} 1 - t^2 & -2t \\ 2t & 1 - t^2 \end{pmatrix}$$

and let  $T$  denote an indeterminate. Observe that

$$f^{g(T)} = f \quad (4.6)$$

because  $F$  is infinite and  $f$  is an invariant of  $SO(2, F)$ . Let  $r_i = (C_{i1} \ C_{i2})$  and observe that the following identities hold:

$$|r_i r_j|^{g(T)} = |r_i r_j|, \quad (4.7)$$

$$\langle r_i, r_j \rangle^{g(T)} = \langle r_i, r_j \rangle, \quad (4.8)$$

$$\begin{aligned} |r_i e_1|^{g(T)} &= -C_{i2}^{g(T)} \\ &= \left( \frac{2T}{1 + T^2} \right) |r_i e_2| + \left( \frac{1 - T^2}{1 + T^2} \right) |r_i e_1|, \end{aligned} \quad (4.9)$$

$$\begin{aligned} |r_i e_2|^{g(T)} &= C_{i1}^{g(T)} \\ &= \left( \frac{1 - T^2}{1 + T^2} \right) |r_i e_2| - \left( \frac{2T}{1 + T^2} \right) |r_i e_1|. \end{aligned} \quad (4.10)$$

Let  $(M, W)$  denote a standard  $SO(2)$ -tableau and define  $\hat{M}$  as in the proof of Proposition 11. Equations (4.7)–(4.10) imply that

$$\begin{aligned} (|M\rangle\langle W|)^{g(T)} &= \left(\frac{2T}{1+T^2}\right)^{e_1(M)} \left(\frac{1-T^2}{1+T^2}\right)^{e_2(M)} |\hat{M}\rangle\langle W| \\ &+ \sum_{i \geq 0} \sum_{0 \geq j \geq -(e_1(M) + e_2(M))} h_{ij} T^i (1+T^2)^j, \end{aligned} \quad (4.11)$$

where  $h_{ij} \in F[C, m \times 2]$  for all  $i, j$  and the leading monomials of the  $h_{ij}$ 's are strictly less than the leading monomial of  $|\hat{M}\rangle\langle W|$ .

Set

$$\begin{aligned} E &= \max\{e_1(M_1) + e_2(M_1), \dots, e_1(M_k) + e_2(M_k)\}, \\ J &= \{j: e_2(M_j) = E\} \end{aligned}$$

and

$$J' = \{j: e_2(M_j) = E - 1 \text{ and } e_1(M_j) = 1\}.$$

Since the  $SO(2)$ -tableau  $(M_j, W_j)$  is standard for all  $j$ ,  $e_1(M_j) = 0$  or  $1$  for all  $j$ , so the set  $J \cup J'$  is non-empty. Equations (4.5) and (4.11) imply that

if  $E > 0$ , then

$$\begin{aligned} (1+T^2)^E f^{g(T)} &= 2^E \sum_{j \in J} c_j |\hat{M}_j\rangle\langle W_j| + 2^E T \sum_{j \in J'} c_j |\hat{M}_j\rangle\langle W_j| \\ &+ y + Tz + (1+T^2)h, \end{aligned} \quad (4.12)$$

where  $h$  lies in  $F[C, m \times 2][T]$  and  $y$  and  $z$  are elements of  $F[C, m \times 2]$  whose leading monomials are strictly less than the leading monomial of some element  $|\hat{M}_j\rangle\langle W_j|$ , with  $j \in J \cup J'$ .

Equations (4.6) and (4.12) imply that

if  $E > 0$ , then

$$\begin{aligned} 2^E \sum_{j \in J} c_j |\hat{M}_j\rangle\langle W_j| + y &= 2^E \sum_{j \in J'} c_j |\hat{M}_j\rangle\langle W_j| + z \\ &= 0. \end{aligned} \quad (4.13)$$

Proposition 12 implies that the elements  $|\hat{M}_j\rangle\langle W_j|$ , where  $j$  ranges over  $J$ , have distinct leading monomials. This observation and statement (4.13) imply that

$$\begin{aligned} \text{either } E=0 \text{ or } J \text{ is empty or the leading monomial of } y \text{ is} \\ \text{greater than or equal to the leading monomial of } |\hat{M}_j\rangle\langle W_j| \\ \text{for all } j \text{ in } J. \end{aligned} \quad (4.14)$$

Proposition 12 also implies that the elements  $|\hat{M}_j| \langle W_j \rangle$ , where  $j$  ranges over  $J'$ , have distinct leading monomials. This observation and statement (4.13) imply that

$$\begin{aligned} &\text{either } E=0 \text{ or } J' \text{ is empty or the leading monomial of } z \text{ is} \\ &\text{greater than or equal to the leading monomial of } |\hat{M}_j| \langle W_j \rangle \\ &\text{for all } j \text{ in } J'. \end{aligned} \quad (4.15)$$

The hypothesis on  $y$  and  $z$ , the fact that  $J \cup J'$  is non-empty, and statements (4.14) and (4.15) imply that  $E=0$ . Therefore  $e_1(M_i) = e_2(M_i) = 0$  for all  $i$ . ■

**PROPOSITION 14.** *Let  $F$  denote an infinite field of characteristic different from two. The set of invariants of  $SO(n, F)$  in  $F[C, m \times n]$  equals the  $F$ -algebra generated by the  $n \times n$  minors of  $C_{m \times n}$  and the elements  $C \langle i|j \rangle_n$ , where  $1 \leq i, j \leq m$ .*

*Proof.* Statement (3.3) implies that every  $n \times n$  minor of  $C_{m \times n}$  is an invariant of  $SO(n, F)$  and statement (4.1) implies that  $C \langle i|j \rangle_n$  is an invariant of  $SO(n, F)$  for all  $i, j$ .

Proposition 13 implies that the invariants of  $SO(2, F)$  in  $F[C, m \times n]$  are generated by the  $2 \times 2$  minors of  $C_{m \times 2}$  and the elements  $C \langle i|j \rangle_2$ , where  $1 \leq i, j \leq m$ . Suppose now that  $n > 2$  and let  $L$  denote the leading monomial of an invariant of  $SO(n, F)$ . Proposition 2 implies that  $R_{t, t+1}(L)$  is the leading monomial of an invariant of  $SO(2, F)$  for  $t = 1, 2, \dots, n-1$ . This observation and Propositions 12 and 13 imply that

$$\begin{aligned} &\text{for } t = 1, 2, \dots, n-1, \text{ there is a standard } SO(2)\text{-tableau} \\ &(M_t, W_t) \text{ such that } e_1(M_t) = e_2(M_t) = 0 \text{ and } R_{t, t+1}(L) \text{ is} \\ &\text{the leading monomial of } |M_t| \langle W_t \rangle. \end{aligned} \quad (4.16)$$

Let  $G$  denote the set of minors of  $C_{m \times n} C_{m \times n}^T$  and  $n \times n$  minors of  $C_{m \times n}$ .

*Claim.* Every monomial  $L$  which satisfies condition (4.16) is the leading monomial of a product of elements of  $G$ .

To establish the claim, proceed by induction on the degree of  $L$ . If degree  $L=0$ , then  $L$  is the leading monomial of the empty product of elements of  $G$ . Suppose now that degree  $L > 0$ .

One may write  $L = L_1 L_2 \cdots L_n$ , where  $L_j$  is a monomial in the letters  $C_{1j}, C_{2j}, \dots, C_{mj}$  for all  $j$ . Condition (4.16) implies that

$$\deg L_t - \deg L_{t+1} = \deg \langle W_t \rangle, \quad \text{for all } t < n.$$

Therefore

$$\deg L_t \geq \deg L_{t+1}, \quad \text{for } t = 1, 2, \dots, n-1 \quad (4.17)$$

and

$$\deg L_t - \deg L_{t+1} \text{ is even,} \quad \text{for } t = 1, 2, \dots, n-1. \quad (4.18)$$

Condition (4.16) also implies that

$$\begin{aligned} \text{the number of rows of } M_t \text{ is congruent mod 2 to degree } L_t, & \quad \text{for} \\ t = 1, 2, \dots, n-1. & \quad (4.19) \end{aligned}$$

Let  $u$  denote the biggest subscript such that  $\deg L_u > 0$ . Relation (4.17) implies that  $\deg L_t > 0$  when  $1 \leq t \leq u$ . If  $1 \leq t \leq u$ , let  $a(t)$  denote the smallest positive integer such that  $C_{a(t)t}$  divides  $L_t$ . Condition (4.16) implies that

$$\begin{aligned} \text{if } 1 \leq t < u, \text{ then the first row of } M_t \text{ is} \\ ((C_{a(t)1} C_{a(t)2}) (C_{a(t+1)1} C_{a(t+1)2})). \end{aligned} \quad (4.20)$$

Suppose at first that  $u = n$ . Let  $L'$  denote the monomial such that  $L = C_{a(1)1} C_{a(2)2} \cdots C_{a(n)n} L'$ . For  $t = 1, 2, \dots, n-1$ , let  $M'_t$  denote the matrix which is obtained from  $M_t$  by deleting its first row. Statements (4.16) and (4.20) and the definition of  $L'$  imply that  $R_{t,t+1}(L')$  is the leading monomial of  $|M'_t| \langle W_t \rangle$  for all  $t < n$ . Therefore the induction hypothesis implies that  $L'$  is the leading monomial of a product of elements of  $G$ . Statement (4.20) and the hypothesis that  $M_t$  is standard for all  $t$  imply that  $a(1) < a(2) < \cdots < a(n)$ . Therefore  $C_{a(1)1} C_{a(2)2} \cdots C_{a(n)n}$  is the leading monomial of an  $n \times n$  minor of  $C_{m \times n}$ . Hence  $L$  is the leading monomial of a product of elements of  $G$ .

Suppose now that  $1 \leq u < n$ . Relations (4.18) and (4.19) imply that  $M_t$  has an even number of rows for all  $t$ . Relations (4.16) and (4.17) imply that, when  $1 \leq t < u$ ,  $M_t$  is non-empty. Therefore, when  $1 \leq t < u$ ,  $M_t$  has at least two rows and when  $1 \leq t \leq u$ ,  $\deg L_t \geq 2$ . If  $1 \leq t \leq u$ , let  $b(t)$  denote the smallest integer such that  $C_{a(t)t} C_{b(t)t}$  divides  $L_t$ . Note that

$$\begin{aligned} \text{if } 1 \leq t < u, \text{ then the second row of } M_t \text{ is} \\ ((C_{b(t)1} C_{b(t)2}) (C_{b(t+1)1} C_{b(t+1)2})). \end{aligned} \quad (4.21)$$

Define  $L'$  to be the monomial such that

$$L = C_{a(1)1} C_{b(1)1} C_{a(2)2} C_{b(2)2} \cdots C_{a(u)u} C_{b(u)u} L'.$$

If  $1 \leq t < u$ , let  $M'_t$  denote the matrix which is obtained from  $M_t$  by deleting its first two rows. Let  $V_u$  denote the sequence which is obtained from  $W_u$  by deleting its first two terms. Observe that  $R_{t,t+1}(L')$  is the leading monomial of  $|M'_t| \langle W_t \rangle$  when  $1 \leq t < u$  and  $R_{u,u+1}(L')$  is the leading

monomial of  $\langle V_u \rangle$ . When  $t > u$ ,  $R_{t+1}(L') = 1$ . These observations and the induction hypothesis imply that  $L'$  is the leading monomial of a product of elements of  $G$ . Statements (4.20) and (4.21) and the hypothesis that  $M_t$  is standard for all  $t$  imply that  $a(1) < a(2) < \dots < a(u)$  and  $b(1) < b(2) < \dots < b(u)$ . These inequalities and Proposition 10 imply that  $C_{a(1)1} C_{b(1)1} \dots C_{a(u)u} C_{b(u)u}$  is the leading monomial of a  $u \times u$  minor of  $C_{m \times n} C_{m \times n}^T$ . Therefore  $L$  is the leading monomial of a product of elements of  $G$ . This establishes the claim.

Statement (4.16) and the preceding claim imply that

$$\begin{aligned} & \text{the leading monomial of any invariant of } SO(n, F) \text{ equals the} \\ & \text{leading monomial of a product of minors of } C_{m \times n} C_{m \times n}^T \text{ and} \\ & n \times n \text{ minors of } C_{m \times n}. \end{aligned} \quad (4.22)$$

This statement and Proposition 1 imply that the products of elements of  $G$  span the invariants of  $SO(n, F)$  in  $F[C, m \times n]$ . ■

## 5. INVARIANTS OF THE ORTHOGONAL GROUP OVER AN INFINITE FIELD OF CHARACTERISTIC TWO

Let  $g$  denote an  $n \times n$  orthogonal matrix. Note that, when the characteristic of the scalar field is two,

$$\begin{aligned} & [C_{i1} + C_{i2} + \dots + C_{in} - (C_{i1} + C_{i2} + \dots + C_{in})^g]^2 \\ & = C_{i1}^2 + C_{i2}^2 + \dots + C_{in}^2 - (C_{i1}^2 + C_{i2}^2 + \dots + C_{in}^2)^g \\ & = 0 \quad \text{by statement (4.1).} \end{aligned}$$

This equation and statement (4.1) imply that

$$\begin{aligned} & \text{when the characteristic of } F \text{ is two, the polynomials} \\ & C_{i1} + C_{i2} + \dots + C_{in} \quad \text{and} \quad C_{i1} C_{j1} + C_{i2} C_{j2} + \dots + C_{in} C_{jn} \quad \text{are} \\ & \text{invariants of } O(n, F). \end{aligned} \quad (5.1)$$

For the rest of this section the letter  $F$  denotes an infinite field of characteristic two.

**PROPOSITION 15.** *Every invariant of  $O(2, F)$  in  $F[C, m \times 2]$  is a linear combination of standard products of  $2 \times 2$  minors of*

$$\begin{pmatrix} C_{11} & C_{12} \\ \vdots & \vdots \\ C_{m1} & C_{m2} \\ 1 & 1 \end{pmatrix}.$$

*Proof.* Let

$$H = \begin{pmatrix} C_{11} & C_{12} \\ & \vdots \\ C_{m1} & C_{m2} \\ 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Observe that, for  $i = 1, 2, \dots, m$ ,  $C_{i1}$  and  $C_{i1} + C_{i2}$  are  $2 \times 2$  minors of  $H$ . This observation and the corollary to Proposition 5 imply that every element of  $F[C, m \times 2]$  is a linear combination of standard products of  $2 \times 2$  minors of  $H$ . Therefore, if  $f$  is any non-zero element of  $F[C, m \times 2]$ , there are distinct standard  $H$ -matrices  $M_1, \dots, M_k$  and non-zero scalars  $c_1, \dots, c_k$  such that

$$f = c_1 |M_1| + \dots + c_k |M_k|. \quad (5.2)$$

Since  $\det \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = 1$ , one may assume furthermore that the row  $((1 \ 1)(0 \ 1))$  does not appear in  $M_1$  or  $M_2$  or  $\dots$  or  $M_k$ . This assumption and the assumption that  $M_1, \dots, M_k$  are standard imply that

the first columns of  $M_1, \dots, M_k$  do not contain the entry  $(1 \ 1)$ . (5.3)

For  $j = 1, 2, \dots, k$ , let  $e(j)$  denote the number of appearances of the row vector  $(0 \ 1)$  as an entry of  $M_j$ . To finish the proof it suffices to show that  $e(j) = 0$  for all  $j$  when  $f$  is an invariant of  $O(2, F)$ .

Let  $g(t) = \begin{pmatrix} t & t+1 \\ t & t+1 \end{pmatrix}$  and observe that  $g(t)$  lies in  $O(2, F)$  for all  $t$  in  $F$ . Note that the following identities hold:

$$(C_{i1} + C_{i2})^{g(t)} = C_{i1} + C_{i2}, \quad (5.4)$$

$$(C_{i1} \ C_{j2} - C_{i2} \ C_{j1})^{g(t)} = C_{i1} \ C_{j2} - C_{i2} \ C_{j1}, \quad (5.5)$$

$$C_{i1}^{g(t)} = C_{i1} + t(C_{i1} + C_{i2}). \quad (5.6)$$

Define  $\hat{M}_j$  to be the matrix which is obtained from  $M_j$  by replacing every appearance of the entry  $(0 \ 1)$  with the entry  $(1 \ 1)$ . Equations (5.4), (5.5), and (5.6) imply that one may write

$$|M_j|^{g(t)} = t^{e(j)} |\hat{M}_j| + \sum_{d=0}^{e(j)-1} h_{jd} t^d, \quad (5.7)$$

where the  $h_{jd}$ 's denote elements of  $F[C, m \times 2]$ . Let  $e$  denote the biggest



element of the set  $\{e(1), e(2), \dots, e(k)\}$  and let  $J = \{j: e(j) = e\}$ . Equations (5.2) and (5.7) imply that one may write

$$f^{g(t)} = \left( \sum_{j \in J} c_j |\hat{M}_j| \right) t^e + \sum_{0 \leq i < e} f_i t^i, \quad (5.8)$$

where  $f_0, \dots, f_{e-1}$  denote elements of  $F[C, m \times 2]$ .

Condition (5.3) and the hypothesis that the matrices  $M_1, \dots, M_k$  are distinct standard matrices imply that the matrices  $\hat{M}_j$ , as  $j$  ranges over  $J$ , are distinct standard matrices. Therefore the polynomials  $|\hat{M}_j|$ , as  $j$  ranges over  $J$ , have distinct leading monomials. In particular these polynomials are linearly independent over  $F$ , so

$$\sum_{j \in J} c_j |\hat{M}_j| \neq 0. \quad (5.9)$$

Suppose now that  $f$  is an invariant of  $O(2, F)$ . Note that  $f^{g(t)} = f$  for all  $t$  in  $F$ . This observation, Eqs. (5.8) and (5.9), and the assumption that  $F$  is infinite imply that  $e = 0$ . Therefore  $e(j) = 0$  for all  $j$ . ■

*Notation.* If  $S$  is a set, let  $P(2, S)$  denote the set of unordered partitions of  $S$  into subsets of sizes one or two. For example, if  $S = \{1, 2, 3\}$ , then  $P(2, S)$  consists of the four partitions

$$\begin{aligned} & \{\{1\}, \{2\}, \{3\}\}, \\ & \{\{1, 2\}, \{3\}\}, \\ & \{\{1, 3\}, \{2\}\}, \\ & \{\{1\}, \{2, 3\}\}. \end{aligned}$$

Let  $A$  denote a subset of  $\{1, 2, \dots, m\}$  which has one or two elements. If  $A = \{u\}$ , define

$$C(A, n) = C_{u1} + C_{u2} + \dots + C_{un},$$

and if  $A = \{u, v\}$ , where  $u \neq v$ , define

$$C(A, n) = C_{u1} C_{v1} + C_{u2} C_{v2} + \dots + C_{un} C_{vn}.$$

If  $S$  is a subset of  $\{1, 2, \dots, m\}$ , define

$$M(S, C, n) = \sum_{p \in P(2, S)} \prod_{A \in p} C(A, n).$$

For example,

$$\begin{aligned}
 M(\{1, 2, 3\}, C, n) = & (C_{11} + \cdots + C_{1n})(C_{21} + \cdots + C_{2n})(C_{31} + \cdots + C_{3n}) \\
 & + (C_{11}C_{21} + C_{12}C_{22} + \cdots + C_{1n}C_{2n})(C_{31} + \cdots + C_{3n}) \\
 & + (C_{11}C_{31} + C_{12}C_{32} + \cdots + C_{1n}C_{3n})(C_{21} + \cdots + C_{2n}) \\
 & + (C_{11} + \cdots + C_{1n})(C_{21}C_{31} + C_{22}C_{32} + \cdots + C_{2n}C_{3n}).
 \end{aligned}$$

**PROPOSITION 16.** *Let  $S = \{a, b, \dots, k\}$ , where  $a, b, \dots, k$  is a strictly increasing sequence of positive integers. Let  $s$  denote the number of elements of  $S$ . View the polynomial  $M(S, C, n)$  as an element of  $F[C, k \times n]$  (where  $\text{char. } F = 2$ ); then  $M(S, C, n)$  equals the sum of the  $s \times s$  minors of the matrix*

$$\begin{pmatrix} C_{a1} & C_{a2} & \cdots & C_{an} \\ C_{b1} & C_{b2} & \cdots & C_{nb} \\ & & \vdots & \\ C_{k1} & C_{k2} & \cdots & C_{kn} \end{pmatrix}.$$

*In particular, if  $s > n$  then  $M(S, C, n) = 0$ . If  $s \leq n$  then  $M(S, C, n)$  is non-zero and its leading monomial is  $C_{a1}C_{b2}\cdots C_{ks}$ .*

*Proof.* Let  $u$  and  $v$  be distinct elements of  $S$  and let  $j$  be an element of  $\{1, 2, \dots, n\}$ . For every partition  $p$  in  $P(2, S)$ , let  $p'$  denote the partition which is obtained from  $p$  by interchanging the numbers  $u$  and  $v$ . Observe that, for every monomial  $w$  in  $F[C, k \times n]$  which is divisible by  $C_{uj}C_{vj}$ , the coefficient of  $w$  in the polynomial  $\prod_{A \in p} C(A, n)$  equals the coefficient of  $w$  in the polynomial  $\prod_{A \in p'} C(A, n)$ . This observation and the hypothesis that the characteristic of  $F$  is two imply that

for every monomial  $w$  which is divisible by  $C_{uj}C_{vj}$ , the

$$\text{coefficient of } w \text{ in } \sum_{\substack{p \in P(2, S) \\ p \neq p'}} \prod_{A \in p} C(A, n) \text{ is zero in } F. \quad (5.10)$$

Observe that  $p = p'$  if and only if the partition  $p$  contains either the set  $\{u, v\}$  or the sets  $\{u\}$  and  $\{v\}$ . Hence

$$\begin{aligned}
 & \sum_{\substack{p \in P(2, S) \\ p = p'}} \prod_{A \in p} C(A, n) \\
 &= (C(\{u, v\}, n) + C(\{u\}, n)C(\{v\}, n))M(S - \{u, v\}, C, n). \quad (5.11)
 \end{aligned}$$

Observe that, for every monomial  $w$  which is divisible by  $C_{uj} C_{vj}$ , the coefficient of  $w$  in  $C(\{u, v\}, n) M(S - \{u, v\}, C, n)$  is the same as the coefficient of  $w$  in  $C(\{u\}, n) C(\{v\}, n) M(S - \{u, v\}, C, n)$ . This observation and statements (5.10) and (5.11) imply that

none of the monomials appearing in  $M(S, C, n)$  are divisible by  $C_{uj} C_{vj}$ . (5.12)

Let  $j_1, j_2, \dots, j_s$  denote distinct elements of  $\{1, 2, \dots, n\}$  and let  $p$  be an element of  $P(2, S)$ . Observe that the coefficient of  $C_{aj_1} C_{bj_2} \dots C_{kj_s}$  in  $\prod_{A \in p} C(A, N)$  is one if  $p = \{\{a\}, \{b\}, \dots, \{k\}\}$  and is zero otherwise. This observation and statement (5.12) imply that

$$M(S, C, n) = \sum_f C_{af(a)} C_{bf(b)} \dots C_{kf(k)}, \quad (5.13)$$

where the sum ranges over all one-to-one functions  $f$  from  $S$  to  $\{1, 2, \dots, n\}$ . Note that the sum is empty when  $s > n$ ; hence  $M(S, C, n) = 0$  when  $s > n$ . When  $s \leq n$ , Eq. (5.13) implies that the leading monomial of  $M(S, C, n)$  is  $C_{a_1} C_{b_2} \dots C_{k_s}$ . Equation (5.13) and the hypothesis that the characteristic of  $F$  is two imply that  $M(S, C, n)$  equals the sum of the  $s \times s$  minors of

$$\begin{pmatrix} C_{a_1} & C_{a_2} & \dots & C_{a_n} \\ & \vdots & & \\ C_{k_1} & C_{k_2} & \dots & C_{k_n} \end{pmatrix}.$$

COROLLARY.  $M(S, C, n)^2 = C\langle a, b, \dots, k | a, b, \dots, k \rangle_n$ .

*Proof.* Let  $A$  denote the matrix which is mentioned in Proposition 16, and observe that  $C\langle a, b, \dots, k | a, b, \dots, k \rangle_n = \det(AA^T)$ . The Binet–Cauchy formula [9, p. 9] implies that

$$\begin{aligned} \det(AA^T) &= \sum_d d^2, & \text{where the sum ranges over all } s \times s \text{ minors of } A \\ &= \left( \sum_d d \right)^2 & \text{since char. } F = 2. \end{aligned}$$

Proposition 16 implies that  $M(S, C, n) = \sum_d d$ . Therefore

$$C\langle a, b, \dots, k | a, b, \dots, k \rangle_n = M(S, C, n)^2. \quad \blacksquare$$

PROPOSITION 17. *The set of invariants of  $O(n, F)$  in  $F[C, m \times n]$  equals the  $F$ -algebra generated by the set  $\{C_{i1} + C_{i2} + \dots + C_{in}, C_{i1} C_{j1} + C_{i2} C_{j2} + \dots + C_{in} C_{jn} : 1 \leq i, j \leq m\}$ .*

*Proof.* The proposition is easy to verify when  $n = 1$ . Assume that  $n \geq 2$  and let  $L$  denote the leading monomial of an invariant of  $O(n, F)$ . Observe that the standard products of  $2 \times 2$  minors of

$$\begin{pmatrix} C_{11} & C_{12} \\ & \vdots \\ C_{m1} & C_{m2} \\ 1 & 1 \end{pmatrix}$$

have distinct leading monomials. This observation and Propositions 2 and 15 imply that

for  $t = 1, 2, \dots, n-1$ , there is a standard  $\begin{pmatrix} C_{11} & C_{12} \\ & \vdots \\ C_{m1} & C_{m1} \\ 1 & 1 \end{pmatrix}$ -matrix

$M_t$  such that  $R_{t,t+1}(L)$  is the leading monomial of  $|M_t|$ . (5.14)

Let  $G = \{M(S, C, n): S \subseteq \{1, 2, \dots, m\}\}$ .

*Claim.* If  $L$  is a monomial which satisfies condition (5.14), then  $L$  is the leading monomial of a product of elements of  $G$ .

To establish the claim, proceed by induction on the degree of  $L$ . If degree  $L = 0$ , then  $L$  is the leading monomial of the empty product of elements of  $G$ . Suppose now that degree  $L > 0$  and that  $L$  satisfies condition (5.14). One may write  $L = L_1 L_2 \cdots L_n$ , where  $L_j$  is a monomial in the letters  $C_{1j}, C_{2j}, \dots, C_{mj}$  for all  $j$ . Condition (5.14) implies that

$$\text{degree } L_1 \geq \text{degree } L_2 \geq \cdots \geq \text{degree } L_n. \quad (5.15)$$

Let  $u$  denote the biggest integer such that degree  $L_u > 0$ . Relation (5.15) implies that if  $1 \leq j \leq u$ , then degree  $L_j > 0$ . For  $j = 1, 2, \dots, u$ , let  $a(j)$  denote the smallest positive integer such that  $C_{a(j)j}$  divides  $L_j$ . Condition (5.14) implies that

$$\text{If } 1 \leq j < u, \text{ then the first row of } M_j \text{ is } ((C_{a(j)1} C_{a(j)2}) (C_{a(j+1)1} C_{a(j+1)2})) \text{ and if } u < n, \text{ then the first row of } M_u \text{ is } ((C_{a(u)1} C_{a(u)2}) (1 \ 1)). \quad (5.16)$$

Let  $L'$  denote the monomial such that  $L = C_{a(1)1} C_{a(2)2} \cdots C_{a(u)u} L'$  and let  $v = \text{minimum } \{u, n-1\}$ . If  $1 \leq j \leq v$ , let  $M'_j$  denote the matrix which is obtained from  $M_j$  by deleting its first row. Condition (5.16) implies that, for  $t = 1, 2, \dots, v$ ,  $R_{t,t+1}(L')$  is the leading monomial of  $|M'_t|$ . Note also that

$R_{t+1}(L') = 1$  when  $v < t < n$ . Therefore the induction hypothesis implies that  $L'$  is the leading monomial of a product of elements of  $G$ . Proposition 16 implies that  $C_{a(1)1} C_{a(2)2} \cdots C_{a(u)u}$  is the leading monomial of  $M(\{a(1), \dots, a(u)\}, C, n)$ . Therefore  $L$  is the leading monomial of a product of elements of  $G$ . This establishes the claim.

Statement (5.14) and the preceding claim imply that

the leading monomial of any invariant of  $O(n, F)$  in  $F[C, m \times n]$  equals the leading monomial of a product of elements in  $\{M(S, C, n): S \subseteq \{1, 2, \dots, m\}\}$ . (5.17)

Every element of  $G$  lies in the algebra generated by elements of the form  $C_{i1} + \cdots + C_{in}$  and  $C_{i1} C_{j1} + \cdots + C_{in} C_{jn}$ . Therefore statement (5.1) implies that every element of  $G$  is an invariant of  $O(n, F)$ . Statement (5.17) and Proposition 1 imply that the products of elements of  $G$  span the space of invariants of  $O(n, F)$  in  $F[C, m \times n]$ . ■

## 6. THE SECOND FUNDAMENTAL THEOREM

**DEFINITION.** Let  $f$  denote a non-zero polynomial in several indeterminates. Write  $f = f_0 + f_1 + \cdots + f_d$ , where  $f_j$  denotes either zero or a homogeneous polynomial of degree  $j$ . Let  $i$  denote the smallest subscript such that  $f_i \neq 0$ ; then the initial form of  $f$  is defined to be  $f_i$ .

**PROPOSITION 18** [21, pp. 74 and 76–77].

(i) The  $n^2$  elements  $\langle i|j \rangle_n$ , where  $1 \leq i, j \leq n$ , are algebraically independent over  $F$ .

(ii) The  $n(n+1)/2$  elements  $C\langle i|j \rangle_n$ , where  $1 \leq i \leq j \leq n$ , are algebraically independent over  $F$ .

*Proof* (S. Mulay). Let  $\delta_{ij}$  denote the  $(i, j)$ th entry of the  $n \times n$  identity matrix. Let  $h$  denote the  $F$ -algebra homomorphism from  $F[C, n \times n; X, n \times n]$  to  $F[C, n \times n]$  such that  $h(C_{ij}) = C_{ij}$  and  $h(X_{ij}) = \delta_{ij}$  for all  $i, j$ . Observe that  $h(\langle i|j \rangle_n) = C_{ij}$  for all  $i, j$ , so the elements  $h(\langle i|j \rangle_n)$  are algebraically independent over  $F$ . Therefore the elements  $\langle i|j \rangle_n$  are algebraically independent over  $F$ . This establishes statement (i).

Now let  $h$  denote the  $F$ -algebra endomorphism of  $F[C, n \times n]$  such that  $h(C_{ij}) = C_{ij} + \delta_{ij}$  when  $i \leq j$  and  $h(C_{ij}) = 0$  when  $i > j$ . To finish the proof, it suffices to show that the elements  $h(C\langle i|j \rangle_n)$ , where  $1 \leq i \leq j \leq n$ , are algebraically independent over  $F$ . Let  $g(Y)$  denote a non-zero element of  $F[Y_{ij}: 1 \leq i \leq j \leq n]$  and let  $g_I(Y)$  denote its initial form.

Suppose at first that the characteristic of  $F$  is not two. If  $i \leq j$ , then the initial form of  $h(C\langle i|j\rangle_n) - \delta_{ij}$  is  $(1 + \delta_{ij}) C_{ij}$ , so

$$g(h(C\langle i|j\rangle_n) - \delta_{ij}) = g((1 + \delta_{ij}) C_{ij}) + \text{a linear combination of forms of higher degrees.}$$

The elements  $(1 + \delta_{ij}) C_{ij}$ , where  $1 \leq i \leq j$ , are algebraically independent, so  $g(h(C\langle i|j\rangle_n) - \delta_{ij}) \neq 0$ . This proves that the elements  $h(C\langle i|j\rangle_n)$  are algebraically independent over  $F$ .

Suppose now that the characteristic of  $F$  equals two. Let  $z_{ij} = h(C\langle i|j\rangle_n)$  if  $i < j$  and let  $z_{ii} = C_{ii} + C_{ii+1} + \dots + C_{in}$ . Let  $y_{ij}$  denote the initial form of  $z_{ij}$  and note that

$$g(z_{ij}) = g(y_{ij}) + \text{a linear combination of forms of higher degrees.}$$

Note that the initial form of  $h(C\langle i|j\rangle_n)$  is  $C_{ij}$  when  $i < j$  and the initial form of  $z_{ii}$  is  $z_{ii}$ . Therefore the elements  $y_{ij}$ , where  $1 \leq i \leq j$ , are algebraically independent over  $F$ . Hence  $g(z_{ij}) \neq 0$ , so the elements  $z_{ij}$  are algebraically independent over  $F$ . This observation and the fact that  $z_{ii}^2 = h(C\langle i|i\rangle_n) + 1$  imply that the elements  $h(C\langle i|j\rangle_n)$  are algebraically independent over  $F$ . ■

**PROPOSITION 19.** (i) *The leading monomial of any element of  $F[\langle a|b\rangle_n; 1 \leq a \leq m, 1 \leq b \leq p]$  equals the leading monomial of a product of minors of  $C_{m \times n} X_{p \times n}^T$ .*

(ii) *The leading monomial of any element of  $F[C\langle a|b\rangle_n; 1 \leq a \leq m, 1 \leq b \leq m]$  equals the leading monomial of a product of minors of  $C_{m \times n} C_{m \times n}^T$ .*

*Proof.* Let  $A_n = F[\langle a|b\rangle_n; 1 \leq a \leq m, 1 \leq b \leq p]$  and let  $C^D X^E$  denote the leading monomial of an element of  $A_n$ . Since  $C^D X^E$  is a monomial which appears in an element of  $A_n$ ,  $\text{degree } C^D = \text{degree } X^E$ . Relation (3.16) implies that there are polynomials  $g_1, g_2$ , and  $g_3$  such that  $g_1$  is a product of  $n \times n$  minors of  $C_{m \times n}$ ,  $g_2$  is a product of  $n \times n$  minors of  $X_{p \times n}$ ,  $g_3$  is a product of minors of  $C_{m \times n} X_{p \times n}^T$ , and the leading monomial of  $g_1 g_2 g_3$  equals  $C^D X^E$ . This statement and the fact that  $\text{degree } C^D = \text{degree } X^E$  imply that  $\text{degree } g_1 = \text{degree } g_2$ . Therefore Proposition 3 implies that the leading monomial of  $g_1 g_2$  equals the leading monomial of a product of  $n \times n$  minors of  $C_{m \times n} X_{p \times n}^T$ . Hence  $C^D X^E$  is the leading monomial of a product of minors of  $C_{m \times n} X_{p \times n}^T$ .

Let  $B_n = F[C\langle a|b\rangle_n; 1 \leq a \leq m, 1 \leq b \leq m]$  and let  $L$  denote the leading monomial of an element of  $B_n$ . One may write  $L = L_1 L_2 \dots L_n$ , where  $L_j$  denotes a monomial in the letters  $C_{1j}, C_{2j}, \dots, C_{mj}$  for all  $j$ . Since  $L$  is a monomial which appears in an element of  $B_n$ , the degree of  $L_j$  is even for all  $j$ .

Assume at first that the characteristic of  $F$  is not two. By statement (4.22) there are polynomials  $g_1$  and  $g_2$  such that  $g_1$  is a product of minors of  $C_{m \times n} C_{m \times n}^T$ ,  $g_2$  is a product of  $n \times n$  minors of  $C_{m \times n}$ , and the leading monomial of  $g_1 g_2$  is  $L$ . Since the degree of  $L_1$  is even,  $g_2$  must be a product of an even number of  $n \times n$  minors of  $C_{m \times n}$ . Therefore Proposition 10 implies that the leading monomial of  $g_2$  equals the leading monomial of a product of minors of  $C_{m \times n} C_{m \times n}^T$ . Therefore  $L$  is the leading monomial of such a product.

Assume now that the characteristic of  $F$  equals two. Statement (5.17) implies that  $L$  is the leading monomial of a product of elements of the form  $M(S, C, n)$ , where  $S \subseteq \{1, 2, \dots, m\}$ . Therefore Proposition 16 and the fact that the degree of  $L_j$  is even for all  $j$  imply that there are subsets  $S_1, S_2, \dots, S_k, T_1, T_2, \dots, T_k$  of  $\{1, 2, \dots, m\}$  such that the size of  $S_j$  equals the size of  $T_j$  for all  $j$  and  $L$  equals the leading monomial of  $\prod_j M(S_j, C, n) M(T_j, C, n)$ . Propositions 10 and 16 imply that the leading monomial of  $M(S_j, C, n) M(T_j, C, n)$  equals the leading monomial of a minor of  $C_{m \times n} C_{m \times n}^T$  for every  $j$ . Therefore  $L$  is the leading monomial of a product of minors of  $C_{m \times n} C_{m \times n}^T$ . ■

It is also possible to prove Proposition 19 without using any results about the covariants of  $SL(n, F)$  or the invariants of  $SO(n, F)$ . For example, statement (i) can be proved as follows. The case  $n=2$  can be established by using Propositions 3 and 5 and the fact that the values of standard  $SL(2)$ -triples have distinct leading monomials. Suppose now that  $n \geq 2$  and let  $L$  denote the leading monomial of an element of  $A_n$  (where  $A_n = F[\langle a|b \rangle_n : 1 \leq a \leq m, 1 \leq b \leq p]$ ).

*Claim.* For  $t = 1, 2, \dots, n-1$ ,  $R_{t+1}(L)$  is the leading monomial of an element of  $A_2$ .

To establish the claim, proceed by induction on  $n$ . The case  $n=2$  is easily seen to be true, so assume that  $n > 2$ . One may write

$$f = \sum_r f_r u_r = \sum_s g_s v_s,$$

where the  $f_r$ 's denote elements of  $A_{n-1}$ , the  $u_r$ 's denote distinct monomials in  $F[C_{in} X_{jn} : 1 \leq i \leq m, 1 \leq j \leq p]$ , the  $g_s$ 's denote distinct monomials in  $A_1$ , and the  $v_s$ 's denote elements of  $F[C_{i2} X_{j2} + C_{i3} X_{j3} + \dots + C_{in} X_{jn} : 1 \leq i \leq m, 1 \leq j \leq p]$ . Note that there exist subscripts  $R$  and  $S$  such that

$$L = \text{the leading monomial of } f_R u_R = \text{the leading monomial of } g_S v_S.$$

These equations and the induction hypothesis imply that  $R_{t+1}(L)$  is the leading monomial of an element of  $A_2$  for  $t = 1, 2, \dots, n-1$ . This establishes the claim.

The claim and the case  $n=2$  of the proposition imply that, for  $t=1, 2, \dots, n-1$ ,  $R_{t,t+1}(L)$  is the leading monomial of a product of minors of  $C_{m \times 2} X_{p \times 2}^T$ . Therefore the proof of Proposition 4 shows that  $L$  is the leading monomial of a product of minors of  $C_{m \times n} X_{p \times n}^T$ .

**PROPOSITION 20** (The Second Fundamental Theorem of Vector Invariants for the General Linear Group). *Let  $Y_{m \times p} = (Y_{ij})$  denote an  $m \times p$  matrix of commuting indeterminates. Let  $h_n$  denote the  $F$ -algebra homomorphism from  $F[Y_{ij}; 1 \leq i \leq m, 1 \leq j \leq p]$  to  $F[C, m \times n; X, p \times n]$  such that  $h_n(Y_{ij}) = \langle i|j \rangle_n$  for all  $i, j$ . The kernel of  $h_n$  is generated as an ideal by the  $(n+1) \times (n+1)$  minors of  $Y_{m \times p}$ .*

*Proof.* Proposition 3 implies that every  $(n+1) \times (n+1)$  minor of  $Y_{m \times p}$  lies in the kernel of  $h_n$ .

Set  $N = \text{maximum}\{m, p\}$ . If  $n \geq N$ , then Proposition 18(i) implies that the map  $h_n$  is one-to-one; hence the proposition holds in this case. Suppose now that  $n < N$ . Proposition 18(i) implies that the map  $h_N$  is one-to-one. Let  $B$  denote a set of products of minors of  $C_{m \times N} X_{p \times N}^T$  such that the elements of  $B$  have distinct leading monomials and such that the leading monomial of any product of minors of  $C_{m \times N} X_{p \times N}^T$  equals the leading monomial of an element of  $B$ . Propositions 1 and 19(i) imply that the set  $B$  spans the  $F$ -algebra generated by the entries of  $C_{m \times N} X_{p \times N}^T$ . Let  $A$  denote this  $F$ -algebra, and let  $f$  denote a non-zero element of the kernel of  $h_n$ . Since  $B$  spans  $A$ , one may write  $h_n(f) = c_1 b_1 + \dots + c_t b_t$ , where  $b_1, \dots, b_t$  are distinct elements of  $B$  and  $c_1, \dots, c_t$  are non-zero scalars.

Suppose that  $b \in B$ . Proposition 3 implies that when  $h_n(h_N^{-1}(b)) \neq 0$ , it has the same leading monomial as  $b$ . Hence the non-zero elements in  $\{h_n(h_N^{-1}(b)); b \in B\}$  have distinct leading monomials, so they are linearly independent over  $F$ . Note also that

$$0 = h_n(f) = c_1 h_n(h_N^{-1}(b_1)) + \dots + c_t h_n(h_N^{-1}(b_t));$$

therefore  $h_n(h_N^{-1}(b_i)) = 0$  for  $i=1, 2, \dots, t$ . This observation and Proposition 3 imply that, for  $i=1, 2, \dots, t$ , there is an integer  $k(i) > n$  such that  $b_i$  is divisible by a  $k(i) \times k(i)$  minor of  $C_{m \times N} X_{p \times N}^T$ . Thus  $h_n(f)$  lies in the  $A$ -ideal generated by the  $(n+1) \times (n+1)$  minors of  $C_{m \times n} X_{p \times n}^T$ . This observation and the fact that  $h_n$  is one-to-one imply that  $f$  lies in the ideal generated by the  $(n+1) \times (n+1)$  minors of  $Y_{m \times p}$ . ■

At this point I would like to make some comments about the Basis Theorem for bideterminants; this theorem can be found, for example, in [6, p. 72], and the terminology in [6, pp. 66–68] will be used here. Let  $h_n$  denote the  $F$ -algebra homomorphism from the letter place algebra to  $F[C, m \times n; X, p \times n]$  such that  $h_n((x_i|u_j)) = \langle i|j \rangle_n$  for all  $i, j$ . Observe that



the images under  $h_n$  of standard bideterminants of shape no longer than  $(n)$  have distinct leading monomials. This observation proves that standard bideterminants are linearly independent; it also proves, when combined with the Basis Theorem for bideterminants, Propositions 18(i), 19(i), and 20. Hence these propositions may be viewed as corollaries of the Basis Theorem. Conversely, the Basis Theorem can be deduced easily from Propositions 18(i) and 19(i), as follows. It has already been shown that the standard bideterminants are linearly independent. By Proposition 18(i), there is an integer  $n$  for which  $h_n$  is one-to-one. Let  $(T|T')$  denote a bideterminant; without loss of generality we assume that the entries in every row of  $T$  and  $T'$  are strictly increasing. By permuting the entries in each column of  $[T, T']$ , one can obtain a standard bitableau  $[U, U']$ , and the leading monomial of  $h_n((U|U'))$  must be the same as that of  $h_n((T|T'))$ . Therefore Proposition 19(i) implies that every non-zero element in the image of  $h_n$  has the same leading monomial as an element of the form  $h_n((U|U'))$ , where  $[U, U']$  is standard. Hence Proposition 1 implies that the vector space spanned by the elements  $h_n((U|U'))$ , where  $[U, U']$  is standard, equals the image of  $h_n$ . Therefore, since we may choose  $n$  so that  $h_n$  is one-to-one, the standard bideterminants span the letter place algebra.

**PROPOSITION 21** (The Second Fundamental Theorem of Vector Invariants for the Orthogonal Group over a Field of Characteristic Different from Two). *Let  $\{Y_{ij}; 1 \leq i \leq j \leq m\}$  denote a set of commuting indeterminates and let  $M$  denote the  $m \times m$  symmetric matrix whose  $(i, j)$ th entry is  $Y_{ij}$  when  $1 \leq i \leq j \leq m$ . Let  $h_n$  denote the  $F$ -algebra homomorphism from  $F[Y_{ij}; 1 \leq i \leq j \leq m]$  to  $F[C, m \times n]$  such that  $h_n(Y_{ij}) = C\langle i|j \rangle_n$  for all  $i, j$ . The kernel of  $h_n$  is generated as an ideal by the  $(n+1) \times (n+1)$  minors of  $M$ .*

*Proof.* Suppose at first that  $m \leq n$ . Proposition 18(ii) implies that the map  $h_n$  is one-to-one, so the proposition holds. Suppose now that  $m > n$ . Proposition 10 implies that every  $(n+1) \times (n+1)$  minor of  $M$  lies in the kernel of  $h_n$ . Proposition 18(ii) implies that the map  $h_m$  is one-to-one.

Let  $A$  denote the  $F$ -algebra generated by the elements  $C\langle i|j \rangle_m$ , where  $1 \leq i \leq j \leq m$ . Let  $B$  denote a set of products of minors of  $C_{m \times m} C_{m \times m}^T$  such that the elements of  $B$  have distinct leading monomials and such that the leading monomial of any product of minors of  $C_{m \times m} C_{m \times m}^T$  equals the leading monomial of an element of  $B$ . Propositions 1 and 19(ii) imply that the set  $B$  spans  $A$ . Let  $f$  denote a non-zero element of the kernel of  $h_n$ , and write  $h_m(f) = c_1 b_1 + \cdots + c_t b_t$ , where  $b_1, \dots, b_t$  are distinct elements of  $B$  and  $c_1, \dots, c_t$  are non-zero scalars.

Suppose that  $b \in B$ . Proposition 10 implies that when  $h_n(h_m^{-1}(b)) \neq 0$ , it has the same leading monomial as  $b$ . Hence the non-zero elements in

$\{h_n(h_m^{-1}(b)): b \in B\}$  have distinct leading monomials, so they are linearly independent over  $F$ . Note also that  $0 = h_n(f) = c_1 h_n(h_m^{-1}(b_1)) + \cdots + c_t h_n(h_m^{-1}(b_t))$ ; therefore  $h_n(h_m^{-1}(b_i)) = 0$  for  $i = 1, 2, \dots, t$ . This observation and Proposition 10 imply that, for  $i = 1, 2, \dots, t$ , there is an integer  $k(i) > n$  such that  $b_i$  is divisible by a  $k(i) \times k(i)$  minor of  $C_{m \times m} C_{m \times m}^T$ . Therefore  $h_m(f)$  lies in the  $A$ -ideal generated by the  $(n+1) \times (n+1)$  minors of  $C_{m \times m} C_{m \times m}^T$ . This remark and the fact that  $h_m$  is one-to-one imply that  $f$  lies in the ideal generated by the  $(n+1) \times (n+1)$  minors of  $M$ . ■

Note that the preceding proposition holds for fields  $F$  of arbitrary characteristic.

*Notation.* Let  $i$  and  $j$  denote positive integers. Define  $Y(\{i\}) = Y_{ii}$  and, if  $i < j$ , define  $Y(\{i, j\}) = Y_{ij}$ . If  $S$  is any subset of  $\{1, 2, \dots, m\}$ , define

$$w(Y, S) = \sum_{p \in P(2, S)} \prod_{T \in p} Y(T).$$

**PROPOSITION 22.** *Let  $h_n$  denote the  $F$ -algebra homomorphism from  $F[Y_{ij}: 1 \leq i \leq j \leq m]$  to  $F[C, m \times n]$  such that  $h_n(Y_{ii}) = C_{i1} + C_{i2} + \cdots + C_{in}$  for all  $i$  and  $h_n(Y_{ij}) = C \langle i | j \rangle_n$  for all  $i < j$ . If the characteristic of  $F$  is two, then the kernel of  $h_n$  is generated as an ideal by the elements  $w(Y, S)$ , where  $S$  ranges over all subsets of  $\{1, 2, \dots, m\}$  of sizes greater than  $n$ .*

*Proof.* Assume that the characteristic of  $F$  is two. Observe that  $(C_{i1} + C_{i2} + \cdots + C_{in})^2 = C \langle i | i \rangle_n$ . This equation and Proposition 18(ii) imply that when  $m \leq n$ , the map  $h_n$  is one-to-one. Therefore the proposition holds when  $m \leq n$ . Suppose now that  $m > n$ . Proposition 18(ii) implies that  $h_m$  is one-to-one. Let  $A$  denote the image of  $h_m$ . Statement (5.17) implies that the leading monomial of any element of  $A$  equals the leading monomial of a product of elements of the form  $M(S, C, m)$ , where  $S \subseteq \{1, 2, \dots, m\}$ .

Let  $B$  denote a set of products of elements of the form  $M(S, C, m)$  such that the elements of  $B$  have distinct leading monomials and the leading monomial of any element of  $A$  equals the leading monomial of an element of  $B$ . Proposition 1 implies that  $B$  spans  $A$ . Let  $f$  denote a non-zero element of the kernel of  $h_n$  and write  $h_m(f) = c_1 b_1 + \cdots + c_t b_t$ , where  $b_1, \dots, b_t$  are distinct elements of  $B$  and  $c_1, \dots, c_t$  are non-zero scalars. Proposition 16 implies that the non-zero elements in  $\{h_n(h_m^{-1}(b)): b \in B\}$  have distinct leading monomials, so they are linearly independent over  $F$ . Note also that  $0 = h_n(f) = c_1 h_n(h_m^{-1}(b_1)) + \cdots + c_t h_n(h_m^{-1}(b_t))$ , so  $h_n(h_m^{-1}(b_i)) = 0$  for  $i = 1, 2, \dots, t$ . This observation and Proposition 16 imply that, for  $i = 1, 2, \dots, t$ , there is a subset  $S_i$  of  $\{1, 2, \dots, m\}$  such that the size of  $S_i$  is strictly greater than  $n$  and  $b_i$  is divisible by  $M(S_i, C, m)$ . Thus  $h_m(f)$  lies in the  $A$ -ideal generated by elements of the form  $M(S, C, m)$ , where  $S$  has

more than  $n$  elements. This statement and the fact that  $h_m$  is one-to-one imply that  $f$  lies in the ideal generated by elements of the form  $w(Y, S)$ , where  $S$  has more than  $n$  elements. Proposition 16 implies that if  $S$  has more than  $n$  elements, then  $w(Y, S)$  lies in the kernel of  $h_n$ . ■

**PROPOSITION 23.** (The Second Fundamental Theorem of Vector Invariants for the Orthogonal Group over a Field of Characteristic Two). *Assume that the characteristic of  $F$  is two and define  $h_n$  as in Proposition 22. The kernel of  $h_n$  is generated as an ideal by the elements  $w(Y, S)$ , where  $S$  ranges over all subsets of  $\{1, 2, \dots, m\}$  of sizes  $n+1$  or  $n+2$ .*

*Proof.* Let  $S$  denote a subset of  $\{1, 2, \dots, m\}$  with at least two elements. Let  $s$  denote the smallest element of  $S$  and observe that

$$w(Y, S) = \sum_{j \in S} Y_{sj} w(Y, S - \{s, j\}).$$

This equation implies that, if  $|S| > 2$ , then

$w(Y, S)$  lies in the ideal generated by the set

$$\{w(Y, T): T \text{ has } |S| - 1 \text{ or } |S| - 2 \text{ elements}\}. \quad (6.1)$$

Repeated applications of statement (6.1) imply that if  $S$  is any subset of  $\{1, 2, \dots, m\}$  such that  $|S| > n$ , then  $w(Y, S)$  lies in the ideal generated by the set  $\{w(Y, T): |T| = n+1 \text{ or } n+2\}$ . This observation and Proposition 22 finish the proof. ■

## ACKNOWLEDGMENTS

I am grateful to G.-C. Rota for his encouragement of this work. I am grateful to J. Kung for furnishing me with Ref. [18]. I am also grateful to S. Mulay for telling me about his proof of Proposition 18 and permitting me to describe it here.

## REFERENCES

1. S. ABHYANKAR, Combinatoire des tableaux de Young, variétés déterminantielles et calcul de fonctions de Hilbert (written up by A. Galligo), *Rend. Sem. Mat. Univ. Politec. Torino* **42**, 3 (1984), 65–88.
2. M. BARNABEI AND A. BRINI, An elementary proof of the first fundamental theorem of vector invariant theory, *J. Algebra* **102** (1986), 556–563.
3. A. CLEBSCH, "Theorie der binären algebraischen Formen," Teubner, Leipzig, 1872.

4. C. DECONCINI, D. EISENBUD, AND C. PROCESI, Young diagrams and determinantal varieties, *Invent. Math.* **56** (1980), 129–165.
5. C. DECONCINI AND C. PROCESI, A characteristic-free approach to invariant theory, *Adv. in Math.* **21** (1976), 330–354.
6. J. DÉARMÉNEN, J. P. S. KUNG, AND G.-C. ROTA, Invariant theory, Young bitableaux and combinatorics, *Adv. in Math.* **27** (1978), 63–92.
7. J. A. DIEUDONNÉ AND J. B. CARREL, Invariant theory, old and new, *Adv. in Math.* **4** (1970), 1–80 and Academic Press, New York/London, 1971.
8. P. DOUBILET, G.-C. ROTA, AND J. STEIN, On the foundations of combinatorial theory. IX. Combinatorial methods in invariant theory, *Stud. Appl. Math.* **53** (1974), 185–216.
9. F. R. GANTMACHER, “The Theory of Matrices,” Vol. I, Chelsea, New York, 1959.
10. R. GARDNER, The fundamental theorem of vector relative invariants, *J. Algebra* **36** (1975), 314–318.
11. P. GORDAN, “Vorlesungen über Invariantentheorie” (G. Kerschensteiner, Ed.), Vols. I, II, Teubner, Leipzig, 1885, 1887.
12. J. H. GRACE AND A. YOUNG, “The Algebra of Invariants,” Cambridge Univ. Press, Cambridge, 1903.
13. M. HOCHSTER AND J. A. EAGON, Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci, *Amer. J. Math.* **93** (1971), 1020–1058.
14. W. V. D. HODGE, Some enumerative results in the theory of forms, *Proc. Cambridge Philos. Soc.* **39** (1942), 22–30.
15. J. IGUSA, On the arithmetic normality of the Grassmann variety, *Proc. Nat. Acad. Sci. U.S.A.* **40** (1954), 309–313.
16. J. P. S. KUNG AND G.-C. ROTA, The invariant theory of binary forms, *Bull. Amer. Math. Soc. (N.S.)* **10** (1984), 27–85.
17. K. R. MOUNT, A remark on determinantal loci, *J. London Math. Soc.* **42** (1967), 595–598.
18. E. PASCAL, Sopra le relazioni che possono sussistere identicamente fra formazioni simboliche del tipo invariantivo nella teoria generale delle forme algebriche, *Rom. Acc. Lincei Mem.* **V** (1888), 375–387.
19. C. PROCESI, “A Primer of Invariant Theory” (notes by G. Boffi), Brandeis Lecture Notes 1, Waltham, MA, 1982.
20. H. W. TURNBULL, “The Theory of Determinants, Matrices, and Invariants,” Blackie, London, 1931.
21. H. WEYL, “The Classical Groups,” Second edition, Princeton Univ. Press, Princeton, NJ, 1946.
22. A. YOUNG, On quantitative substitutional analysis (third paper), *Proc. London Math. Soc.* **2**, 28 (1927), 255–292.